奇安信天眼威胁监测与分析系统
产品技术白皮书

创建时间：2020 年 1 月 1 日

修改时间：2024 年 10 月 23 日

地址：北京市西城区西直门外南路26号院1号

邮编：100044

修订记录

版本	状态	修订理由和内容摘要	修订人	批准人	修订日期
V1.0	A		葛成宇		2020.5.8
V3.0.10.0	M	变更主体产品名称	葛成宇		2021.7.20
V3.0.11.0.SP5	M	1、产品版本更新到 V3.0.11.0.SP5 2、增加国产化内容	葛成宇		2022.9.29

状态：C-创建，A-增加，M-修改，D-删除

目 录

1 引言

近年来，具备国家和组织背景的 APT 攻击日益增多，例如：美国国家安全局（NSA）对西北工业大学的特定入侵、海莲花组织在 2021 年的攻击频率达到历史之最、2022 年俄乌网络战争等安全事件，2022 年 APT 攻击的主要目标是政府及医疗卫生行业，中国依旧是全球 APT 活动的首要地区性目标，网络窃密活动与网络破坏活动持续加剧，中国数字化转型期间网络安全正在经受着前所未有的巨大考验。

2022 年初，奇安信威胁情报中心发布了《中国高级持续性威胁（APT）2021 年报告》。报告中指出：

(1) 政府和医疗卫生行业成为全球 APT 活动关注的首要目标。全球 41%的 APT 活动事件与政府和医疗卫生行业相关。针对疫控与防疫机构、病毒研究机构、疫苗研发机构和其他相关医学研究机构的高级威胁活动持续不断

(2) 中国继续成为全球 APT 活动的重点地区性目标。针对中国领先的科研机构、科技企业的网络窃密活动与网络破坏活动持续加剧

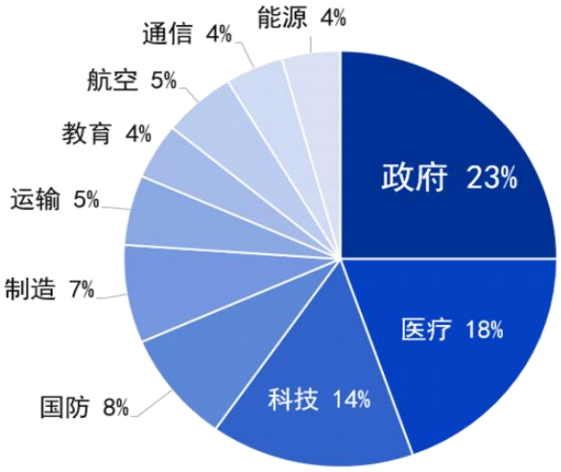


图 1 全球 APT 组织关注领域分布

（2）高级威胁活动涉及目标的国家和地域分布情况统计如下图，可以看到高级威胁攻击活动几乎覆盖了全球绝大部分国家和区域。

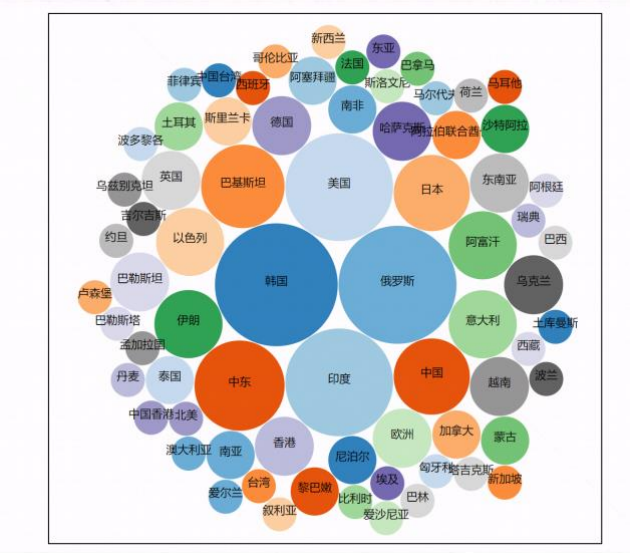


图 2 全球 APT 组织地域分布

（2）奇安信公司累计监测到针对中国境内目标发动攻击的境内外 APT 组织 50 个，通过研究报告等形式，对外披露了包括海莲花（越南）、美人鱼（中东）、摩诃草（印度）、蔓灵花（印度）、黄金眼（国内）等多个由 奇安信命名的 APT 组织。并将数十万高精准失陷类情报不断应用到产品的检测能力中。

2012 年 4 月起至今，某境外黑客组织对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。该组织主要通过鱼叉攻击和水坑攻击等方法，配合多种社会工程学手段进行渗透，向境内特定目标人群传播免杀木马程序，秘密控制部分政府人员、外包商和行业专家的电脑系统，窃取系统中相关领域的机密资料。根据该组织的某些攻击特点，奇安信公司将其命名为 OceanLotus（海莲花），海莲花组织在 2021 年的攻击频率达到历史之最，同时在不断的更新攻击手法。

传统安全防御体系的设备和产品遍布网络 2~7 层的数据分析。其中，与 APT 攻击相关的 7 层设备主要是 IDS、IPS、审计，而负责 7 层检测 IDS、IPS 采用经典的 CIDF 检测模型，该模型最核心的思想就是依靠攻击特征库的模式匹配

完成对攻击行为的检测。反观 APT 攻击，其采用的攻击手法和技术都是未知漏洞（0day）、未知恶意代码等未知行为，在这种情况下，依靠已知特征、已知行为模式进行检测的 IDS、IPS 在无法预知攻击特征、攻击行为模式的情况下，理论上就已无法检测 APT 攻击。

APT 攻击通常都会在内网的某个角落留下蛛丝马迹，但攻击者也会想尽办法清除作案痕迹，为安全防御和侦破工作带来诸多不便。传统的安全事件分析思路是遍历各个安全设备的告警日志，尝试找出其中的关联关系。但在实战过程中，尤其是攻击者采用某些技术手段进行证据销毁工作后，依靠传统的分析方式、传统安全设备通常都无法对 APT 攻击的各个阶段进行有效的检测，也就无法产生相应的告警，安全人员花费大量精力进行告警日志分析往往都是徒劳无功。换个角度来看攻防实战，真相往往隐藏在网络的流量中，那么如果采用全流量采集的思路，会带来以下几个问题：一方面是存储不方便，每天产生的全流量数据会占用过多的存储空间，组织通常没有足够的资源来支撑长时间的存储；另一方面是全流量数据包含了结构化数据、非结构化数据，涵盖了视频、图片、文本等等多种格式，无法直接进行格式化检索，安全人员也就无法从海量的数据中找到有价值的信息。

在安全形势不断恶化的今天，政府、军队、金融、大型企业等客户所处的特殊位置，经常会面临来自互联网的攻击威胁，如何在攻防实战中充分发挥安全防御的价值，越来越成为安全人员所关注的重点；实战化攻防场景在安全体系如何搭建，实战化攻防经验在 HW 过程中如何传递，实战化攻防场景中红队常用哪些攻击战术和攻击手段，蓝队应对攻击常用的战术战略，如何在攻防实战或演习中提升自身的安全能力……

安全的对抗是动态的过程，业务在发展，网络在变化，技术在革新，人员在更替，网络安全绝不是一劳永逸的工作，虽然企业的安全管理人员已经在网络中的各个位置部署了大量的安全设备，但仍然会有部分威胁绕过所有防护直达企业内部，对重要数据资产造成泄漏、

损坏或篡改等严重损失。在实战攻防对抗中，监测分析是返现攻击行为的主要方式，在第一时间发现攻击行为，可为应对提供及时支撑、为响应处置争取充足时间，因此企业需要在其网络中部署威胁感知产品，及时发现潜藏在其网络中的安全威胁，对威胁的恶意行为实现早期的快速发现，对受害目标及攻击源头进行精准定位，对入侵途径及攻击者背景的研判与溯源，从源头上解决企业网络中的安全问题，尽可能地减少安全威胁对企业带来的损失。

2 产品介绍

奇安信天眼威胁监测与分析系统（以下简称“天眼”）汇集流量传感器、文件威胁鉴定器、邮件告警、天堤防火墙、网神云锁等多种告警数据，基于奇安信自有的多维度海量互联网数据，进行自动化挖掘与云端关联分析，提前洞悉各种安全威胁，并向客户推送定制的专属威胁情报；同时结合部署在客户本地的软、硬件设备，奇安信天眼能够对未知威胁的恶意行为实现早期的快速发现，并可对受害目标及攻击源头进行精准定位，最终达到对入侵途径及攻击者背景的研判与溯源；支持运用奇安信自研的 SOAR 编排技术，实现对确定的威胁进行多种类型的响应处置，真正实现监测预警、威胁检测、溯源分析和响应处置的天眼威胁监测与分析系统。

2.1 产品设计目标

2.1.1 解决企业对未知威胁检测和行为分析的问题

传统的 APT 防护技术专注于从企业客户自身流量和数据中通过沙箱或关联分析等手段发现威胁。由于企业网络防护系统缺少相关 APT 学习经验，而且攻击者的逃逸水平也在不断的进步发展，本地设备会经常性的出现误报和漏报现象，经常需要人工的二次分析进行筛选。同时因 APT 攻击的复杂性和背景的特殊性，仅依赖于单一企业的数据经常无法有效的发现 APT 攻击背景，难以做到真正的追踪溯源。

天眼系统创新性的从互联网数据进行发掘和分析，用威胁情报的形式对各种攻击中常出现的特点和背景信息进行记录和传输，所以从互联网进行挖掘攻击线索可极大提升未知威胁和 APT 攻击的检出效率。基于广阔的数据覆盖面，天眼系统的威胁检测和行为分析有了足够的数据基础，可以做到更精准的攻击溯源，极大程度上解决了企业对未知威胁检测和行为分析的难题。

2.1.2 解决企业多元数据无法融合的难题

企业在信息安全建设过程中会部署大量的安全设备，如防火墙、入侵检测/防御设备、各类传感器、流量清洗系统、终端防护系统以及各种安全防护平台。随着建设的逐步深入，各类安全设备种类愈来愈多、数量愈来愈大，反而给安全防护工作带来诸多不便，比如大量设备的海量告警无从下手辨别真伪，真实告警重复报告无法去重，确定的告警事件不知如何处置等等。

天眼系统提供告警统一接收能力，进一步加强告警数据的融合，支持与多种设备免密跳转，在收集数据的同时支持快速跳转功能，便于用户进行设备维护、状态查看等操作，解决企业多元数据无法融合和设备维护不便的难题。

2.1.3 解决网络流量数据实时采集、分析、存储及回溯的难题

传统的安全事件分析思路是遍历各个安全设备的告警日志，尝试找出其中的关联关系。但在实战过程中，尤其是攻击者采用某些手段进行证据销毁工作后，依靠传统的分析方式、传统安全设备通常都无法对 APT 攻击的各个阶段进行有效的检测。而且，通常情况下存在以下难点，一方面是存储不方便，每天产生的全流量数据会占用过多的存储空间，另一方面是全流量数据包含了结构化数据、非结构化数据及多种格式的数据，无法直接进行格式化检索，安全人员也就无法从海量的数据中找到有价值的信息。

换个角度来看攻防实战，真相往往隐藏在网络的流量中，天眼系统采用网络流量实时采集的思路，可以实现基于流量的威胁行为的实时采集与分析，有效解决了未知威胁的发现难题。天眼系统配套的全包存储组件，能提供灵活的存储能力扩展，能对网络原始数据进行全流量完整保存，能对外秒级提取海量历史流量，还原网络事件发生时的全部网络通讯内容，实现数据包级的数据取证和责任判定，在解决海量数据全包存储的同时保证了威胁事件溯源的及时性与准确性。从综合的维度上解决了企业网络流量数据实时采集、分析、存储及回溯的难题。

2.1.4 解决未知恶意文件检测的问题

目前传统的文件检测大多使用基于签名特征库匹配的机制，面对恶意代码的复杂性和多样性，传统的静态检测技术体现出了局限性，已无法完全检测新出现的恶意代码。

为解决此问题，天眼系统通过静态检测和动态检测相结合的形式，通过动态执行对文件进行细粒度的行为检测，能够从行为层面进行细致分析，精准全面分析文件属性，解决用户对未知恶意文件检测的需求。

2.1.5 解决威胁发现精准度不高的问题

高价值告警通常被淹没在海量告警中，合理降低告警数量的同时提供高质量告警一直是安全运营痛点，天眼流量传感器通过对威胁通道的全面覆盖、自主研发的威胁检测引擎、基于双向会话检测机制、语义分析检测技术、智能分析引擎及机器学习等一系列技术，对攻击结果再次精细化提炼，在有效缓解海量告警的同时提升了告警的精准度，使用户能聚焦高价值威胁事件的分析及运营。

2.1.6 解决资产脆弱性发现的难题

当前企业客户所拥有的资产日益增多，资产漏洞及带来的风险隐患也日益增加，如何发现资产脆弱性成为一大难题。

天眼系统将资产与流量相结合，根据告警和流量行为日志数据对资产漏洞和合规性进行分析，进行资产精准度脆弱性和配置核查发现，解决企业资产脆弱性发现不准确、误报率高的难题。

2.1.7 解决威胁分析过程可视化的难题

传统的防护设备只能对攻击行为进行告警，虽然可能会发现很多问题，但无法向用户呈现或描述整个攻击过程。

天眼依据多年积累的经验从攻击链的维度将攻击行为进行重新划分，对告警进行深度调查分析，以告警中的受害主机为线索还原整个攻击过程（侦察-入侵-命令控制-横向渗透-数据外泄-痕迹清理），并结合安全专家积累的经验给出相应的处置方案。天眼系统运用先进的可视化呈现技术，可以将威胁攻击的全过程推演并呈现在用户面前，有效解决了威胁分析过程可视化的难题。

2.1.8 解决响应处置环节脱节的问题

目前，市场上大多数安全产品都可以实现不同程度的威胁检测及告警，但对于识别到的告警如何快速有效的进行处置则显得较为薄弱，通常情况下都是靠人工干预的方式记住某些攻击 IP 或者受害 IP，登录到防火墙、杀毒系统等平台进行手动处置，该方式的响应处置复杂度高、效率低，且容易因误操作导致更为严重的安全事件。

针对此种情况，天眼系统通过内置的自动化编排响应模型，通过与处置设备联动，支持自动/手动方式的响应指令下发，解决响应处置与威胁分析脱节的问题。

2.1.9 解决威胁分析结果可视化难题

企业在信息安全建设过程中虽然部署了大量安全设备和安全防护平台，但通常每个系统都是各自为政，互不兼容，因此在日常运维或特殊演习等场景下无法做到对整体威胁分析结果一目了然的效果。

天眼系统内置多款监控大屏，提供了多个维度、全方位、丰富多彩的整体安全态势展示效果，包括外部威胁态势、威胁事件态势、资产风险态势、访问

态势等，满足了对威胁分析整体状态可视化呈现的需求，解决了分析结果难以可视化呈现的问题。

2.1.10 解决国产化及虚拟化问题

天眼系统满足国产化要求，支持国产服务器（海光芯片）、国产操作系统（麒麟 V10），同时支持云上虚拟化及裸金属（基于麒麟 V10 系统）的虚拟化产品形态。

天眼基于国产海光芯片、麒麟操作系统的国产化方案，可实现产品各性能指标与 INTEL 架构一致、产品维保期间升级版本服务与 INTEL 架构复用系统及引擎规则包的目的。

2.2 产品价值

2.2.1 针对 APT 攻击有效防护

天眼系统内置 ATT&CK 模型和可视化狩猎分析工具，全面助力已知威胁的快速发现和未知威胁的自主拓线分析。同时，天眼系统结合奇安信自研威胁情报系统，通过全貌特征“跟踪”攻击者，持续的发现未知威胁，确保发现的未知威胁的准确性。

天眼流量传感器基于对流量的全量、深度解析，实现对威胁通道的全面覆盖，同时基于天眼自主研发的 QNA 威胁检测引擎，采用 200 多种协议解码 +DPI、SQLparser、NBT 机器学习、webshell 沙箱等底层检测技术实现威胁的全面发现、流式检测、实时告警。基于双向会话检测机制，实现对攻击结果准确判断并进一步区分失陷、成功、失败、企图类攻击结果，为基于威胁的运营方案提供精细化能力支撑。

天眼系统以攻防渗透和数据分析为核心竞争力，聚焦威胁检测和响应，针对 APT 攻击提供有效防护，为客户提供安全服务与产品解决方案，为安全人员

提供一套在监测预警、威胁检测、溯源分析和响应处置上得心应手的威胁检测平台。

2.2.2 针对多元数据的有效整合

天眼系统提供告警统一接收能力，进一步加强告警数据的融合，对传感器、文件威胁鉴定器、邮件威胁检测、网神云锁、终端安全管理系统、天堤智慧分析管理系统的数据进行统一管理，统一字典、统一分析、统一展现，实现多元数据的有效整合展示。同时天眼系统支持与各组件设备间的安全跳转，在收集数据、下发指令的同时支持快速跳转功能，便于用户进行设备维护、状态查看等操作。

2.2.3 针对海量数据的采集、分析和存储及回溯

针对海量数据的采集、分析、存储和回溯，天眼系统采用网络流量实时采集的思路，对于捕获的流量实时匹配传感器规则以及奇安信自研的威胁情报数据，可以实现基于流量的威胁行为的实时采集与分析，有效解决了未知威胁的发现难题。同时，天眼系统配套的全包存储组件，能提供灵活的存储能力扩展，解决了沙箱和传感器在本地对流量进行存储、分析的性能考验问题，间接提升传感器本身的业务性能。并且能对网络原始数据进行全流量完整保存，能对外秒级提取海量历史流量，还原网络事件发生时的全部网络通讯内容，实现数据包级的数据取证和责任判定，在解决海量数据全包存储的同时保证了威胁事件溯源的及时性与准确性。

2.2.4 针对文件的高精准检测

针对文件的高精准检测需求，天眼系统采用基于硬件虚拟化的技术，通过静态检测、动态检测相结合对文件进行全方面过滤分析，结合高精准的奇安信

威胁情报和行为规则，对网络流量中还原的文件实现高精准的未知恶意文件检测，有效避免以文件为载体的未知威胁攻击扩散。

2.2.5 针对威胁发现精准度的提升

天眼基于 HW 实战化经验和长期技术创新及积累，通过智能分析引擎及机器学习对攻击结果再次精细化提炼，在对攻击结果优化、修正的同时可大幅降低海量告警问题，提供高质量的威胁事件告警。

运用语义分析检测技术、后门深度检测算法和极其丰富的模型，基于机器学习检测的方法提升未知威胁检测能力，检测结果也更加准确，同时检测能力标签化，通过为告警注入场景化、ATT&CK 等标签，从源头给威胁分析和溯源赋能。

2.2.6 针对资产脆弱性的发现

针对资产脆弱性发现的问题，天眼系统将资产与流量相结合，根据告警和流量行为日志数据对资产漏洞和合规性进行分析，实现资产脆弱性和配置核查的精准发现。同时，天眼系统对接目前全球最大的漏洞响应平台补天平台，同步有关部门的漏洞库数据，为客户提供实时、高效的漏洞报告与快速响应，全面补齐资产的精准风险预警。

2.2.7 针对威胁分析过程的可视化

天眼依据多年积累的经验从攻击链的维度将攻击行为进行重新划分，对告警进行深度调查分析，以告警中的受害主机为线索还原整个攻击过程（侦察-入侵-命令控制-横向渗透-数据外泄-痕迹清理），并结合安全专家积累的经验给出相应的处置方案。此外，天眼系统运用先进的可视化呈现技术，支持与用户在可视分析画布上对任意线索的自定义拓线及溯源分析，该过程通过一步步的交互对当前数据进行拓线分析，最终可以将威胁攻击的全过程推演并呈现在用

户面前。同时，拓线分析过程支持结果快照导出，对于给定线索的溯源结果进行攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等维度的展示。

2.2.8 针对响应处置的灵活自动化编排

针对实战化场景，天眼系统内置的自动化编排响应模块，通过标准的API/openc2 接口与处置设备联动，连接畅通的情况下支持自动/手动方式的响应指令下发。在天眼自动化编排响应模块中预置多种处置场景应对常见类型的告警事件，对应不同告警事件调用预置的处置流程，通过 API/openc2 接口下发处理动作完成对告警事件的处置，提升业务系统的安全系数。对于非内置场景，天眼响应处置模块同时系统支持通过自主编排功能，根据实际业务需求添加任务脚本、联动服务以及工作流程，实现根据业务需求量身打造处置流程，大大提升了响应处置的速度与准确性，解决响应处置与威胁分析脱节的问题。

2.2.9 针对分析结果的可视化展示

针对实战化场景的可视化，天眼系统内置多款监控大屏，提供了多个维度、全方位、丰富多彩的整体安全态势展示效果，包括外部威胁态势、威胁事件态势、资产风险态势、访问态势等，满足了企业对业务系统整体安全状态可视化呈现的需求。此外，对于用户个性化的可视化展示需求，天眼支持定制方式进行效果呈现。

2.2.10 针对 HW 实战化威胁运营

天眼实战化威胁运营平台以统一的平台连接人、工具和事件，为客户提供集中有效的指挥中心组织结构和响应方案。

实战化威胁运营平台能够有效汇聚和集合各安全设备外发的告警，进行统一分析、研判处置。对于安全事件，通过实战化威胁运营平台组织固化落实到具体任务中，监测、分析、响应处置工作通过平台对应到人，统一调度涉及的

多个部门，共同开展防守工作，在防守期间达到有效的协同来应对网络攻击，构建 ”分工合理“、”责任明确“、”内外结合“的组织结构。实战化威胁运营平台能够协助用户体系化地运用安全技术、安全运营和安全管理手段，持续降低企业或机构的面临的安全风险。

2.3 产品组成与架构

天眼主要功能范围如图所示，包括流量告警采集，威胁检测呈现，溯源分析，联动响应。

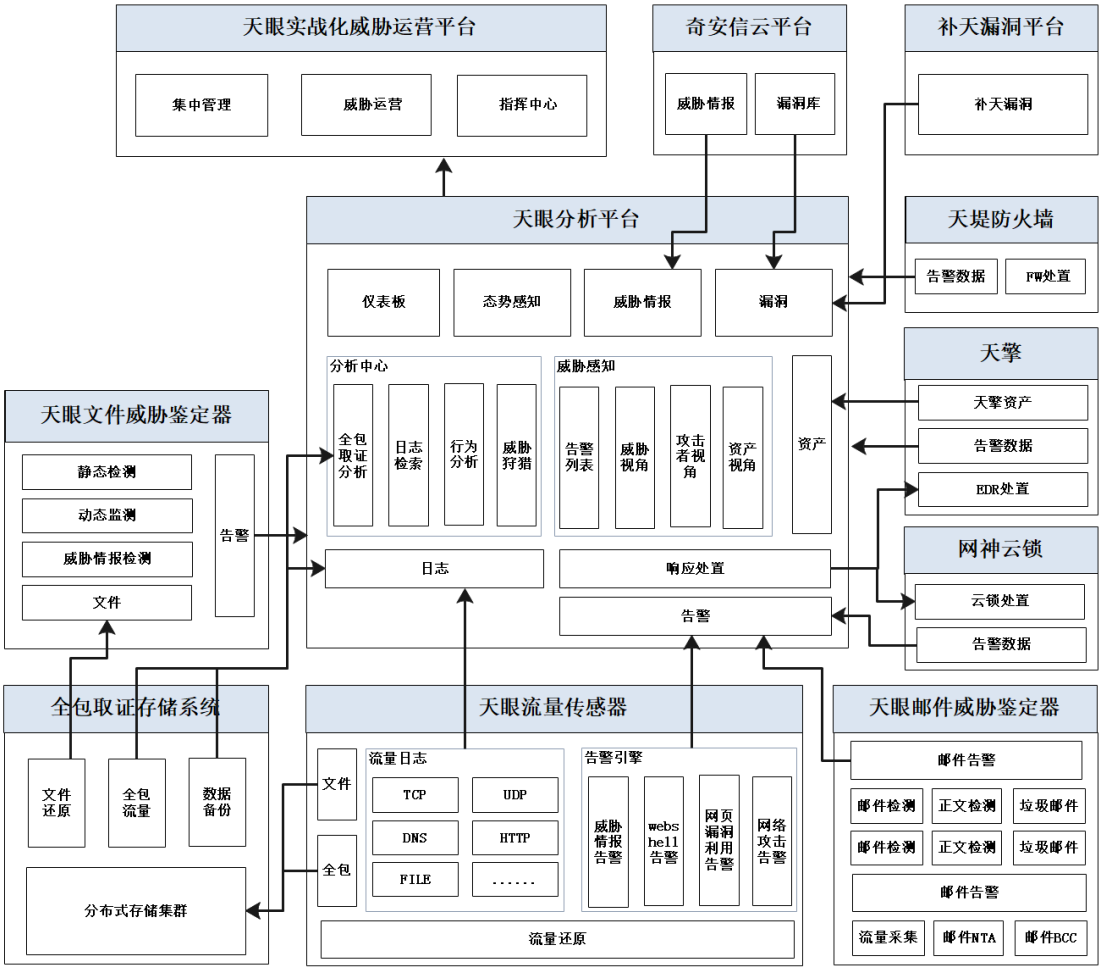


图-1 天眼架构图

天眼流量传感器提供流量采集和告警功能，借助全包存储系统，可以实现全流量存储，并在分析平台上实现全流量回溯分析能力。由流量中还原的文件和邮件数据，经天眼文件威胁鉴定器和天眼邮件威胁鉴定器处理，可进一步触发告警。全包存储系统的引入，使天眼具备对存储灵活扩容的能力。配合云平台、天堤防火墙、天擎 EDR、云锁等系统，天眼具备极强的联动响应能力。天眼分析平台对以上各系统的能力进行综合呈现，为用户提供多维度的威胁分析、呈现和联动响应服务。同时支持把告警上传给天眼实战化威胁运营平台，进行告警的处置、管控、调度。

2.3.1 威胁情报

威胁情报来自奇安信云端的分析成果，可对 APT 攻击、新型木马、特种免杀木马进行规则化描述。奇安信公司依托于云端的海量数据，通过基于人工智能自学习的自动化数据处理技术，依靠以顶尖研究资源为基础的多个国内高水平安全研究实验室为未知威胁的最终确认提供专业高水平的技术支撑，所有大数据分析出的未知威胁都会通过专业的人员进行人工干预，做到精细分析，确认攻击手段、攻击对象以及攻击的目的，通过人工智能结合大数据知识以及攻击者的多个维度特征还原出攻击者的全貌，包括程序形态，不同编码风格和不同攻击原理的同源木马程序，恶意服务器（C&C）等，通过全貌特征‘跟踪’攻击者，持续的发现未知威胁，最终确保发现的未知威胁的准确性，并生成了可供天眼系统使用的威胁情报。

2.3.2 分析平台

天眼分析平台用于存储传感器提交的流量日志、告警日志以及文件威胁鉴定器提交的告警日志。其次天眼分析平台不仅可对所有数据进行快速的处理并为检索提供支持，还能将存储的日志与威胁情报进行碰撞以及进行日志关联性分析产生告警并能在 4K 的屏幕上展示威胁态势，此外天眼分析平台支持对告警进行深度分析，支持以告警字段进行狩猎分析及可视化展示，以攻击链的视角

还原告警中的受害主机被攻击的整个过程。分析平台承担对所有数据进行存储、预处理和检索的工作。由于传统关系型数据库在面对大量数据存储时经常出现性能不足导致查询相关数据缓慢，天眼分析平台底层的数据检索模块采用了分布式计算和搜索引擎技术对所有数据进行处理，可通过多台设备建立集群以保证存储空间和计算能力的供应。结合全包存储系统，分析平台可以实现针对精确告警的全包取证分析和自定义数据包分析能力。

2.3.3 流量传感器

天眼传感器主要负责对网络流量的镜像流量进行采集并还原，还原后的流量日志会加密传输给天眼分析平台，流量镜像中的 PE 和非 PE 文件还原后则加密传输给天眼文件威胁鉴定器进行检测。天眼传感器通过对网络流量进行解码还原出真实流量，提取网络层、传输层和应用层的头部信息，甚至是重要负载信息，这些信息将通过加密通道传送到分析平台进行统一处理。传感器中应用的自主知识产权的协议分析模块，可以在 IPv4/IPv6 网络环境下，支持 HTTP（网页）、SMTP/POP3（邮件）等主流协议的高性能分析。

同时，天眼传感器内置的威胁检测引擎，可检测多种网络协议中的攻击行为，提供网页漏洞利用、webshell 上传、网络攻击、威胁情报多种维度的告警展示，可检测如网络应用、木马、广告、exploit 等多种网络攻击行为，也可检测如 sql 注入、跨站、webshell、命令执行、文件包含等多种 web 攻击行为，内置的 webshell 沙箱和 webshell 机器学习模块可以精准检测 php、asp、jsp 等后门并记录相关信息，拥有威胁情报实时匹配能力，能发现恶意软件、APT 事件等威胁，产生的多种告警都会加密，并传输给天眼分析平台进行统一分析管理。

2.3.4 文件威胁鉴定器

天眼文件威胁鉴定器主要负责对传感器、手动提交、FTP、SMB、URL 等多数据来源通道的样本进行检测。整个检测过程中文件进行威胁情报匹配、沙箱检测、静态检测与动态检测等多种检测，及时发现有恶意行为的文件并告警，告警日志可传给天眼分析平台供统一分析。天眼通过文件威胁鉴定器对文件进行高级威胁检测，文件威胁鉴定器可以接收还原自传感器的大量 PE 和非 PE 文件，使用静态检测、动态检测、沙箱检测等一系列无签名检测方式发现传统安全设备无法发现的高级威胁，并将威胁相关情况以报告行为提供给企业安全管理人员。天眼文件威胁鉴定器上的相关告警也可发送至分析平台实现告警的统一管理和后续的进一步分析。

2.3.5 全包取证存储系统

《新等保 2.0》明确要求支持网络回溯。以前因为没有进行全流量存储，只是对解析出来的流量，存储部分核心字段，如 Payload 只存前 100 字节，导致在进行回溯取证分析时证据不足。新增此模块即满足全包存储需求和应标要求，又可补充丰富天眼威胁检测系统的使用场景，提升竞争力。传感器承担着全流量的采集和存储，以往传感器会把流量存储在本地磁盘，局限于本地磁盘的容量限制，以及带宽限制，空间扩容性差。基于此，需要将全流量进行独立存储，独立维护，独立扩容。做到一端存储，多端访问。因此引进了分布式存储技术。基于分布构建了一个可大规模扩容的存储系统，它可以在单个平台上提供对象级，块级和文件系统级的存储。其特性主要体现在几个方面：

特性丰富：支持块存储、文件系统和对象存储；

高性能：摒弃了传统的集中式存储元数据寻址的方案，采用更加完善的 CRUSH 算法，数据分布均衡，并行度高；

高可用性：副本数可灵活控制，并且考虑了容灾域的隔离，多种故障场景自动进行修复自愈，没有单点故障，自动管理；

高扩展性：采用去中心化的分布式架构，扩展灵活，容量以及性能随节点的增加线性增长。

集群存储能力扩展灵活，可最多扩展至数百台存储服务器达到 PB 级容量和数千个存储客户端。流量吞吐能力取决于集群规模，使用独立单机部署模式，可以最高支持 1Gbps 带宽，使用集群部署模式，最高可以支持 20Gbps 带宽的全包流量采集与检索。

基于全包存储构建的全包取证分析模块可根据用户输入查询条件，或从告警中提取的线索条件，从全流量存储系统提取符合条件的 PCAP 包，并实现类 wireshark 的 PCAP 包解析基本功能。

全包取证分析模块以源 IP、目的 IP、源端口、目的端口作为查询条件，从全包取证系统获取相关会话（PCAP 包形式）。再实现类 WireShark 的功能，对包含目标会话的 PCAP 包进行分析。

全包取证分析可以作为独立功能单独使用，由用户手动输入查询条件，得到目标 PCAP 包，并进行类 WireShark 的会话分析。也可以取告警作为线索入口，以告警包含的 IP 端口信息未查询条件，进行分析。

具体模块如下：

1. 新增全流量包提取功能，展示一段时间内满足查询条件的流量包，并支持下载，同时支持流量趋势展示。

2. 新增全流量包解析功能，展示流量包内的会话列表，及会话协议树信息。

3. 新增告警流量包解析功能，展示告警流量的会话列表，及会话协议树信息。

2.3.6 威胁运营平台

当前客户环境攻防实战化规模越来越大，所覆盖的行业越来越多，传统的方式已经不能满足现在的需求，当前威胁运营的痛点，就是单打独斗，没有统一的平台连接人、工具和事件，并且无集中有效的指挥中心组织结构和响应方案，因此威胁运营平台孕育而生，有效的解决了当前的痛点。

威胁运营平台基于大数据平台架构，平台具有分布式扩展能力，支持软件化部署，分布式计算等；支持对告警、资产、漏洞统一管理，支持本地安全分析服务，威胁大屏展示；支持设备集中管理监控，可以对奇安信设备统一进行系统和情报升级；另外，基于 OpenC2 安全协议和接入设备进行端到端无缝协作；同时，也支持手机端连通协作，实时告警提醒和处置，以及报告接收等；利用平台的强大的运营能力，帮助客户捕获威胁，并快速全面地对威胁进行响应。

3 系统功能介绍

1. 流量威胁检测系统集成了流量传感器、文件威胁鉴定器、邮件告警等多种告警数据源，依托于多维度、海量的互联网数据，实施自动化挖掘与云端关联分析策略，旨在提前洞察各类安全威胁，并为用户提供个性化的威胁情报服务。同时，结合本地部署的软硬件设备，该系统能迅速识别未知威胁的恶意行为，精准定位受害目标及攻击源头，进而实现对入侵途径及攻击者背景的深度研判与溯源。此外，该系统还具备对网络请求语义的分析能力，特别适用于 APT 等高级攻击的检测、分析及溯源工作。

2. 该系统采用分析平台+探针的部署架构，支持分析平台的横向扩展至多台设备集群，以应对不同规模的网络环境。下级分析平台可向上级发送告警及相关信息，便于在上级平台进行统一展示与管理。系统能有效识别各类网络攻击行为，包括但不限于协议异常、代码执行、网络欺骗、漏洞利用、webshell 上传等。同时，支持自定义威胁情报、白名单、弱口令字典、暴力破解规则、

漏洞知识库及自定义规则配置，规则数量不少于 10000 条，可检测的 webshell 类型不少于 170 种。此外，系统还支持特征库及威胁情报库的离线升级，以及基于本地威胁情报库对实时流量的威胁检测，检测范围涵盖 APT 事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具及其他恶意软件。用户可自定义威胁情报，并与云端威胁情报中心联动，实现攻击 IP、C&C 域名及恶意样本 MD5 的一键搜索，获取丰富的相关信息。系统还能对网络请求的语义进行深入分析，展示告警事件的请求头、响应头、请求体及响应体，并提供完整的 pcap 数据包供用户进一步分析。同时，系统能根据上下行流量判断攻击行为是否成功，并将结果直观展示。

3. 该系统支持 B/S 访问架构及国产化 Web 浏览器，提供邮件告警功能，可定时向指定邮箱发送 APT 事件、攻击利用、恶意软件、拒绝服务等类型的告警信息。此外，还支持日志的导入导出、三权分立、资产分组管理及对应内网网段的录入、资产标记、网络日志检索、告警日志检索和终端日志检索等功能，以便深入分析威胁的攻击全过程。特征库和威胁情报库支持在线和离线方式升级。在联动管理方面，系统支持将系统日志、告警日志、原始告警及行为分析信息发送给 syslog 服务器或邮件服务器。同时，探针或分析平台至少有一方支持通过 syslog 将告警日志发送给第三方，并可对发送的事件进行自定义过滤。用户可根据源地址、目的地址、端口、URL、告警名称、XFF 字段等添加白名单，系统还能记录并展示告警 HTTP 头内的 XFF 字段，并支持基于 XFF 字段的搜索匹配。

4. 该系统支持以受害资产为维度进行分析，涵盖失陷状态、受到的攻击类型、威胁级别、攻击阶段及所属资产分组等内容。同时，也能从攻击者维度进行画像分析，包括地理位置信息、国家信息、所属组织、使用的攻击手段及攻击的所有资产等。此外，系统还支持自定义态势展示及从威胁情报、应用安全、系统安全和设备安全等业务场景维度对告警进行攻击带外分析。特别地，系统还能对挖矿行为进行深入分析，并提供威胁情报维度的分析支持。

4 产品核心功能

4.1 流量还原

天眼流量传感器对网络流量进行采集并还原，还原后的流量日志会加密传输给天眼分析平台，流量镜像中的 PE 和非 PE 文件还原后则加密传输给天眼文件威胁鉴定器进行检测。天眼传感器通过对网络流量进行解码还原出真实流量，提取网络层、传输层和应用层的头部信息，甚至是重要负载信息，这些信息将通过加密通道传送到天眼分析平台进行统一处理。天眼传感器中应用的自主知识产权的协议分析模块，可以在 IPv4/IPv6 网络环境下，支持 HTTP （网页）、SMTP/POP3（邮件）等主流协议的高性能分析。

4.2 高级威胁检测

天眼具备高级威胁检测能力。基于全球数百个威胁情报源和奇安信多个安全研究团队的 APT 事件发现、跟踪成果，运用威胁情报、文件虚拟执行、智能规则引擎、机器学习等技术，天眼系统可以检测和发现高级网络攻击和新型网络攻击，涵盖：APT 攻击、勒索软件、远控木马、僵尸网络、窃密木马、间谍软件、网络蠕虫、邮件钓鱼等高级攻击，并基于可视化技术，清晰的展示网络中的威胁。

天眼流量传感器内置的威胁检测引擎，除了高级威胁检测能力之外，还可检测多种网络协议中的攻击行为，提供网页漏洞利用、webshell 上传、网络攻击等多种维度的告警展示，可检测如僵木蠕毒、溢出攻击、拒绝服务、间谍软件、端口扫描、网络钓鱼等多种网络攻击行为，也可检测如 SQL 注入、XSS、Webshell、代码执行、命令执行、文件包含等多种 Web 攻击行为，内置的 Webshell 沙箱和 Webshell 机器学习模块可以精准检测 PHP、ASP、JSP(X)等后门并记录相关信息。

天眼传感器拥有威胁情报实时匹配能力，能发现恶意软件、APT 事件等威胁，产生的多种告警都会加密，并传输给天眼分析平台进行统一分析管理。

4.3 日志检索

天眼基于搜索引擎技术构建流量行为日志检索与存储，在本地数据的存储和检索方面，使用奇安信诺亚大数据平台做为平台基础，并配套了大量的检索和分析功能以对数据做到高效分析。

针对不同使用场景和不同技术水平的用户需求，日志检索模块分为快捷模式、高级模式、专家模式的检索功能，提供告警日志、网络日志、终端日志与第三方日志检索的功能。快捷模式快捷模式只需要填充胶囊字段的值，即可进行基于某一类告警数据的搜索；高级搜索兼容 lucene 语句进行搜索，在输入框内输入查询语句进行基于多种告警数据的搜索；专家模式专家模式为 SPL 命令语句搜索，用于专家用户对数据进行统计并支持各种可视化视图展示。

4.4 响应处置

威胁处置能力在信息安全建设中具有重要作用，天眼系统为完善威胁分析后续的处置闭环，引入了响应处置能力，以模块化形式在天眼系统内置了一套自动化编排响应模型，通过标准的 API/openc2 接口与处置设备联动，连接畅通的情况下支持自动/手动方式的响应指令下发。主要实现的功能是根据告警信息对相应（不同厂商不同功能）的设备构建完整的响应处置工作流进行联动与处置，实现安全设备间的协同防御。

根据不同使用场景，天眼系统响应处置模块提供不同级别的处置手段，主要包括以下场景：

加白名单：针对判定为误报的告警数据，天眼支持以添加白名单形式进行处理，后续产生的告警将不再通知给用户，降低误告警数量，提升事件处置的效率。

深度分析：基于 SOAR 的自动化处置编排能力，天眼响应处置模块结合各类告警和日志进行攻防场景的深度分析，提炼高价值告警和威胁溯源分析拓线，

并将分析结果回注天眼系统生成新的告警。例如，我们基于远控木马的外连 CC 地址行为的威胁情报告警，通过 SOAR 的自动化编排能力来发现外连 CC 地址告警之后是否有持续的与 CC 地址的 TCP 通信行为来判断受害 IP 的受害程度，对于明确有后续通信行为的产生新的告警，这样即实现对告警的深度分析。

联动处置：通过接口与处置设备联动，支持自动/手动方式的响应指令下发，实现对威胁事件的处置动作。天眼内置的响应处置模块支持与多种设备联动：

- EDR 联动

在实际威胁运营过程中，天眼系统通过流量解析发现告警后，支持将告警与 EDR 设备进行联动，完成对某一些进程的封禁、关闭、隔离等操作。

- NDR 联动

在实际威胁运营过程中，天眼系统通过流量解析发现告警后，支持将告警与防火墙设备进行联动，完成对某一 IP 的封禁操作。

- SMAC 联动

在实际威胁运营过程中，天眼系统通过流量解析发现告警后，支持将告警与 SMAC 进行联动，完成对某一 IP 的封禁操作。

- 椒图联动

在实际威胁运营过程中，天眼系统支持接入椒图告警，同时天眼系统通过流量解析发现告警后，支持向椒图下发 IP，椒图可让服务器阻止本 IP 对服务器的响应、支持天眼向椒图下发弱口令排查指令，椒图排查所有服务器相关账号口令是否存在该弱口令并返回扫描结果。

- 传感器旁路阻断

在实际威胁运营过程中，天眼系统通过流量解析发现告警后，基于流量的旁路阻断技术与传感器进行联动，完成对特定 IP、域名的网络访问的阻断操作。

4.5 旁路解密

基于旁路非代理方式解密 HTTPS 流量（需提供私钥），解密后为 HTTP 流量再进行流量还原及威胁分析。

HTTPS 基于 SSL 协议加密，SSL 加密流量主要分为两类，具有前向安全性（DH 算法）和非具有前向安全性（RSA 算法），对于旁路流量，前者不可以解密，后者可以，也就是旁路可解密 RSA 算法，无法解密 DH 算法。

4.6 恶意代码检测

基于人工智能的杀毒引擎，依靠海量数据挖掘、引入机器智能学习算法，能够有效准确识别未知恶意软件，能够根据已知的正常软件和恶意软件的大量样本，通过数据挖掘找出两类软件最具有区分度的特征，建立机器学习模型，使用机器学习算法，得到恶意软件的识别模型。通过获得的模型对未知程序进行分析判断，即可获得软件的恶意概率，从而在可控的误报率之下尽可能多的发现恶意程序。

机器学习引擎的学习流程如下图所示：

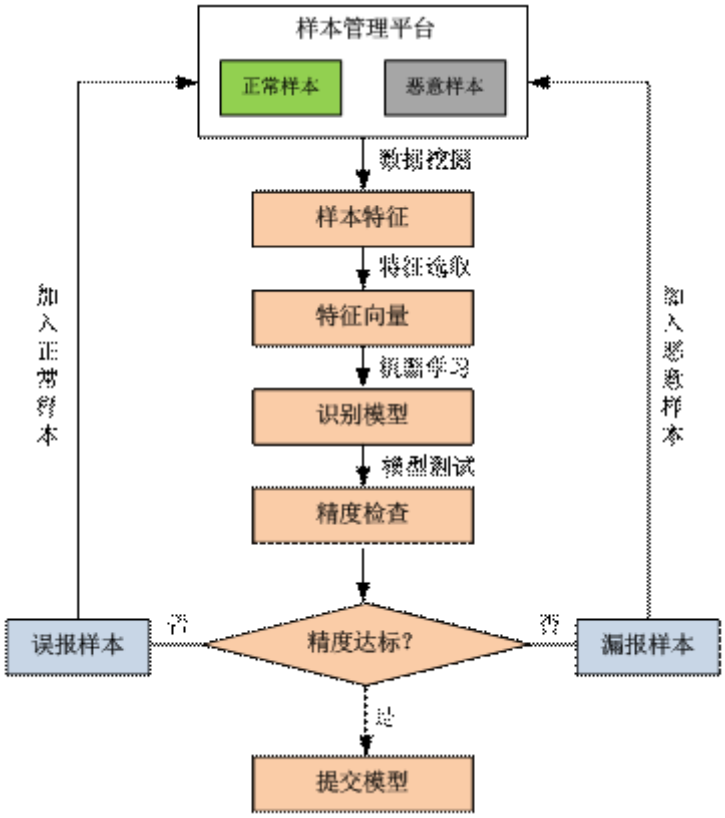


图 2 机器学习引擎流程示意图

样本管理平台负责管理训练样本，并且对可疑样本可进行人工分析，保证训练样本的纯度，并给下面的阶段提供数据。

通过对训练样本的数据挖掘，例如导入 API 函数、PE 头部信息、代码反汇编信息等等进行海量数据挖掘，找到海量 PE 文件特征。应用特征选取算法，选取最有效的特征，建立特征模型。

利用特征模型对训练样本数据进行数据特征化变换，生成对应的特征向量，利用成熟的机器学习算法（例如 SVM），对样本进行训练，得到恶意程序识别问题的识别模型。

对生成的模型进行测试，如果精度达到要求，则终止。否则对误判样本进行分析（在样本不确定的情况下，需要人工分析确认），调整样本的分类属性，再次迭代。

该引擎的运行环境如下图所示：

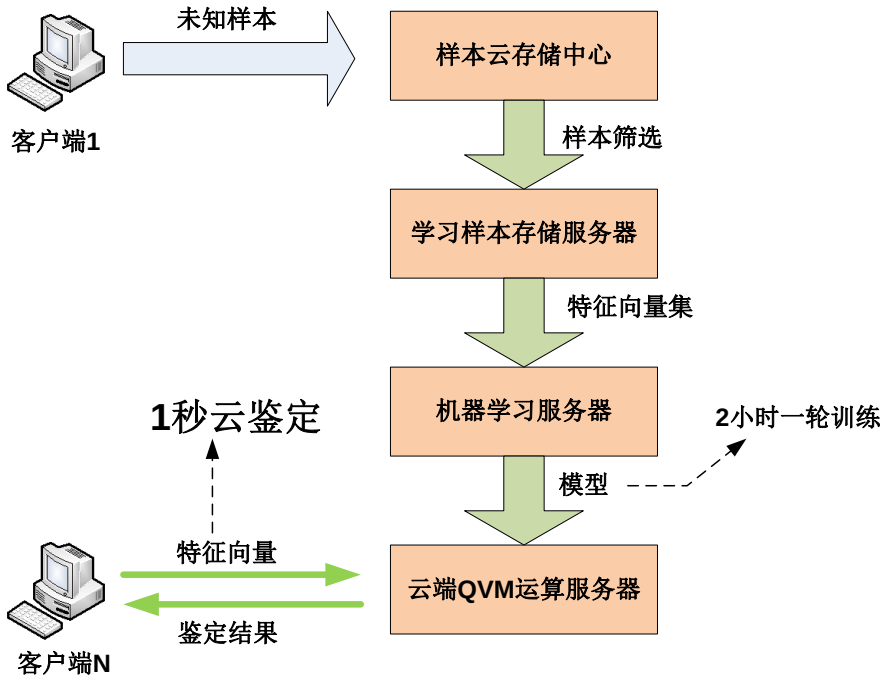


图 3 机器学习引擎运行环境示意图

由于安全领域用户对误报的敏感性和特殊性，导致长期以来机器学习算法在本领域一直作为不大，多数研究者尝试后，无法达到预期的精度而放弃。所以对本技术而言，首要处理的就是降低误报率。根据前期研究的结果，一个合适的机器学习算法的选择对误报控制是相当重要的，目前初选 SVM 作为基本学习算法，并设计了快速的参数选择，和快速训练方法。

机器学习算法在人工少量干预样本（添加、删除、修改黑白属性)指导的情况下，系统能够实现自我学习，自我进化。目前该引擎学习一轮的时间仅为 2 小时。

机器学习有效的解决了大部分未知恶意程序的发现问题。由于传统杀毒技术严重依赖于样本获得能力和病毒分析师的能力，基本只能处理已知问题，不能对可能发生的问题进行防范，具有严重的滞后性和局限性。本技术对海量样

本进行挖掘，能够找到恶意软件的内在规律，能对未来相当长时期的恶意软件技术做出前瞻性预测，实现不更新即可识别大量新型恶意软件。

传统杀毒软件技术基本基于简单的特征或者规则进行查杀，很容易被病毒作者免杀。本算法单特征贡献相当微弱，所以简单免杀很难奏效。

机器学习使得对样本分析人员的要求相对较低，仅仅需要分析员能够区分文件是否恶意，而不需要人工分析恶意软件实现方法和识别方法，降低了人员参与门槛，大大节约了人力成本。

4.7 动态沙箱检测

天眼新一代动态沙箱引擎采用基于硬件模拟的虚拟化动态分析技术，对 APT 攻击的核心环节“恶意代码植入”进行检测，这种利用对恶意代码的行为进行动态分析的方法，可以避免因为无法提前获得未知恶意代码特征而漏检的问题，亦即在无需提前预知恶意代码样本的情况下仍然可以对恶意代码样本进行有效的检测，因为未知恶意代码是 APT 攻击的核心步骤，因此对未知恶意代码样本的有效检测，可以有效解决 APT 攻击过程的检测问题。

新一代安全感知系统相对于最大特点在于：将会提供了非常丰富的沙箱环境，这种规模化的沙箱环境可以有效保障每种待检测的文件样本都有其适合打开、运行的沙箱环境，同时新一代安全感知系统的沙箱采用了高级优化技术，可以有效降低样本文件在沙箱之中打开、运行过程中的内存资源消耗、CPU 资源消耗，与其他同类型产品相比，可以以最小的资源消耗、最快的速度得出准确的检测结果。

目前新一代安全感知系统需要模拟沙箱环境包括：PDF 沙箱、Word 沙箱、浏览器沙箱、邮件沙箱、图片沙箱等。同时，借助于新一代安全感知系统的多核平台，新一代安全感知系统中的各种规模化沙箱可以绑定在处理器的物理核心上进行快速运行，这种进程与处理器绑定的方式可以有效降低进程在处理器

的不同处理核心上切换所带来的资源开销，降低并发检测线程之间的资源竞争，有效提高资源利用率。

4.8 场景化分析

天眼系统基于特定场景的安全威胁分析技术，根据多种威胁类型全面检测用户环境的异常行为，提炼了覆盖全面的行为分析场景，主要包括了 DNS 服务分析、非常规服务分析、邮件行为分析、WEB 服务器行为分析、登录行为分析、数据库行为分析以及访问行为分析等。

- **DNS 服务分析**

DNS 服务分析包括可疑 DNS 分析（DGA 域名检测以及 DNS Tunnel 隧道）、DNS 服务器发现、链路劫持和 DNS 重绑定检测等场景。DGA（域名生成算法）是一种利用随机字符来生成 C&C 域名，从而逃避域名黑名单检测的技术手段。DNS Tunnel 则是黑客可疑利用 DNS 信道来传输数据。链路层劫持是指第三方（可能是运营商、黑客）通过在用户至服务器之间，植入恶意设备或者控制网络设备的手段，侦听或篡改用户和服务器之间的数据，达到窃取用户重要数据（包括用户密码，用户身份数据等等）的目的。DNS 重绑定是指攻击者控制恶意 DNS 服务器来回复域的查询，可以通过滥用 DNS 来诱骗 Web 浏览器与他们不想要的服务器进行通信。

- **非常规服务分析**

非常规服务分析主要完成常规行为分析之外的重要分析任务，包括可疑代理、远程工具和反弹 shell 等行为检测，让用户了解内部资产受到哪些代理工具、远程服务和反弹 shell 的威胁。

服务器转发客户系统的网络访问请求，并且可以过滤掉用户的指令，从而达到控制用户的目的，可疑代理分析为用户提供监测这一威胁的窗口。远程工具，用于主机远程控制，一般分客户端程序(Client)和服务器端程序(Server)两部分，控制端上的 Client 与被控端的 Server 建立连接，完成各种操作。反

弹 shell，表现为控制端监听被控端的 TCP/UDP 端口，被控端发起请求到该端口，并将其命令行的输入输出转到控制端，实现客户端与服务端的角色翻转。这些非常规服务存在潜在威胁，其检测分析任务满足用户需求场景。

- **邮件行为分析**

邮件行为分析场景针对邮件相关威胁所做的安全检测，主要包括检测邮件正文的敏感关键字分析和检测邮件附件的敏感后缀分析。

电子邮件拥有成本低、效率高等特性，已经成为企业通信最重要的形式之一，因此也成为网络攻击者最常攻击的对象，其中包含的恶意信息和恶意软件成为攻击的常见形式。检测恶意信息的方式是匹配敏感关键字，一封邮件存在一定数量的敏感关键字能反映其威胁情况。检测恶意软件的方式是提取邮件附件中的相关敏感后缀，一般是电脑能直接或间接运行的文件格式，过滤掉存在敏感后缀的文件可以在源头控制威胁。

- **登录行为分析**

登录行为分析针对用户登录场景存在的威胁进行相关检测，防止用户账号被恶意控制和窃取密码，分别对应异常登录、特权账号登录，以及弱口令、明文密码泄露。

账号安全是安全控制的最重要一环，针对账号的恶意行为层出不穷，从登录类型和密码检测两个维度可以较全面地检测到登录行为相关异常信息。异常登录分析资产被外网登录和异常时间登录的情况，从源头保护资产。特权账号登录是为了防止攻击者利用特权账号展开攻击，一般包括 administrator 和 root 等，特权账号登录信息的分析能预防潜在威胁。明文密码泄露是检测登录日志中可以被解析的密码，通常存在于 http、smtp 和 pop3 协议中。弱口令分析强度不够或重复次数较多的密码，弱口令的检测是在明文密码泄露的基础上进行的。

- **Web 服务器行为分析**

Web 服务器行为分析包含非常用请求方法、可疑爬虫和扫描和后门上传利用。非常用请求方法是指攻击者经常使用一些不常用的方法来获取服务器的敏感数据为后续的非法活动做准备，我们需要检测非常用的请求来判断是的有信息泄露。可疑爬虫和扫描指攻击者通过网络非法扫描、爬虫等多种攻击来扫描随机生成的 url 和随机方法来获取服务器数据。后门上传利用是指攻击者通过现有漏洞向服务器上传非法文件以获取信息的行为。

- **数据库行为分析**

数据库行为分析是指分析各个用户的语句来获悉用户行为。攻击者的恶意数据库行为包括篡改数据、删除重要数据和盗取数据信息。我们通过分析数据库行为日志，可以分析和获取攻击者的行为。篡改数据是指攻击者修改数据信息致使数据库无法正常使用。删除重要数据是指攻击者删除数据信息致使数据库无法正常使用。盗取数据信息是指攻击者非法获取数据。

- **访问行为分析**

访问行为分析包含外部访问、横向访问、内部主机外联和风险端口访问四类。外部访问是指外部主机访问内部服务；横向访问是指内部主机访问内部服务；内部主机外联是指内部主机访问外部服务的信息；风险端口访问是指通过高危风险端口访问服务器。

行为分析每天要处理海量数据，因此需要采用分布式计算技术，行为分析利用奇安信诺亚大数据平台的分布式特性实现分布式，同时采用了奇安信自研分布式计算框架 Bear 提高程序执行效率。

4.9 SOAR 自动化流程编排

天眼 SOAR 主要为客户提供安全编排与自动化、告警管理、案件管理等功能。它能够帮助企业和组织将繁杂的安全运营（尤其是安全响应）过程梳理为任务和剧本，把分散的安全工具与功能转化为可编程的应用和动作，并且借助编排和自动化技术，将团队、工具和流程的高度协同起来。主要包括：

➢ **安全能力编排化**

通过剧本管理、应用管理、动作管理等功能，将客户分散的安全能力和安全运维响应的过程标准化，形成剧本库和应用库（动作库），实现团队、工具和流程的整合与协同联动。这些标准化流程可以被随时调用，减少了人工的干预，大幅提升应急处置的效率。

➢ **告警响应自动化**

对纷繁的告警信息进行智能分诊，从而自动触发对应流程。一方面告警分诊能够自动化地聚合告警信息，自动计算告警的可信度和处置优先级，帮助管理员聚焦关键的告警；另一方面，告警深度分析还可针对告警信息进行补充调查分析，将低质量的告警变成高质量、有价值的告警，并且排除虚假告警。同时，在进行告警深度分析的同时，运维人员还可对告警进行增强，尽可能清晰、精准地将告警的相关信息呈现出来，方便安全人员进行研判。

➢ **案件管理全程化**

天眼 SOAR 可帮助用户对一组相关的告警进行流程化、持续化的调查分析与响应处置，并且不断积累该案件相关的痕迹物证和攻击者的攻击战术等指标信息。

天眼 SOAR 可帮助客户重点解决因运维响应人员匮乏、安全事件响应不及时、重复性运维工作量大、安全设备之间缺乏协同且联动性差等导致安全运营效率低下的问题，将安全团队、工具和流程真正整合起来，让安全运营工作更加协同一致。

4.10 资产感知

天眼资产管理模块除人工添加资产能力之外，支持通过联动天擎进行资产识别和基于告警的资产发现的能力，通过人工和自动结合的方式对数据进行有效地快速整合与同步，支持告警数据与核心资产的关联分析，有效地解决资产

管理难题。天眼系统资产感知模块整合了资产组管理和网段管理模块，包括资产互访、脆弱性、配置核查和补天漏洞等功能，来对资产的漏洞进行分析。

资产管理模块：支持资产组与资产信息的展示与管理，根据资产 ip 所属网段进行分组，支持增删改查，新增手动添加资产组时对于网段区间的匹配，支持批量导入，支持系统自动根据用户录入的网段发现资产信息。

资产发现模块：支持展示天擎发现的资产详情信息，支持自动从流量中识别资产信息，支持用户审核和编辑，并可以选择忽略某些信息，同时允许用户关闭告警流量发现资产。

资产互访模块：统计资产之间互访的次数和流量，并展示互访的次数、流量和方式等具体信息。

脆弱性模块：展示资产的漏洞信息，其中漏洞来源分为告警来源和配置来源，告警来源即从告警中发现的漏洞信息，配置来源即从行为日志中与用户上传的漏洞知识库进行比对产生的漏洞信息，并根据资产权重、漏洞等级、漏洞数、漏洞次数计算漏洞风险值，并展示 top10 漏洞资产。

配置核查模块：展示行为分析中三种与资产相关的配置类型信息。分别为弱口令、明文密码泄露和风险端口暴露，并根据同一个资产统计出现的三种配置类型的总和进行排序，展示 top10 的配置核查资产。

补天漏洞模块：支持配置连接补天平台，展示来自补天平台的漏洞信息，当系统提示存在企业漏洞，用户可直接登录补天平台，查看漏洞修复方案，及时进行漏洞处置。

4.11 报表报告

天眼系统报表报告模块主要包括快速报表、周期报表及报表模板三个能力，在新建报表任务时可新增过滤条件，在导出生成的报表文件时，增加文件导出类型以及增加新的报表模板。

快速报表、周期报表模块支持自定义配置新增快速或周期报表，支持配置报表格式（新增 HTML 格式的导出文件类型）、报表模板等信息，其中新建周期报表任务时，支持配置攻击维度、威胁级别、告警类型、资产分组、资产 IP、安全事件分析六类过滤条件，支持快速报表任务支持自定义时间过滤。

报表模板部分，提供多种报表模版（支持用户自定义模版），包括告警、受害资产、日志、威胁分析等，并新增天眼分析报告模板，用于展示失陷事件和尝试攻击事件的详情。

4.12 第三方日志接入

为支持第三方设备日志接入，天眼系统通过集成奇安信诺亚平台实现了数据采集、数据处理、数据存储及日志接入模块的管理和监控内容。

诺亚平台的数据采集、数据处理、数据存储构成第三方日志接入运行平台，完成数据接入并存储到系统，数据采集是整个环节的最前端，完成多种不同类型、不同协议数据的采集封包并发送到下一个环节；数据处理模块完成格式化、富化等操作，将不同来源的数据归一化到业务需要的格式；数据存储则完成数据最终的存储动作，控制数据的保存位置、形式，根据不同的业务需求，数据还可以分发一份到流处理，处理完的结构再进入存储。

集成了诺亚平台第三方日志接入模块的天眼系统，支持接入奇安信安全设备日志、第三方安全设备日志、网络设备日志、数据库日志、Windows 主机系统日志、Linux 主机系统日志、Web 服务器日志、虚拟化平台日志、其他日志；日志类型包括 SNMP Trap 日志、文本格式日志、数据库日志、WMI 日志、Netflow 日志、Syslog 日志等，并进行数据解析、入库、展示。

4.13 告警日志外发

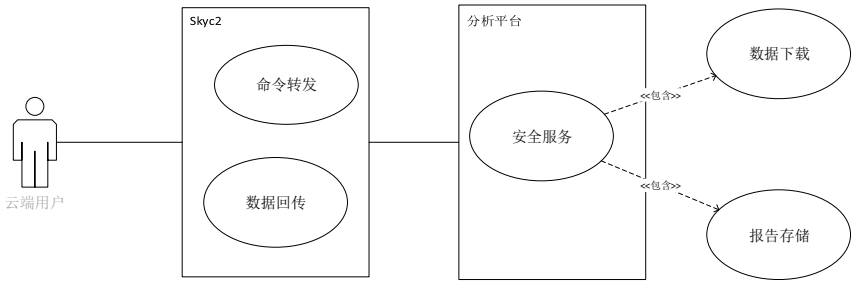
为满足企业用户不同安全管理系统之间数据同步的场景，天眼系统提供告警联动能力，支持通过 SYSLOG、SNMP、邮件、KAFKA 等多种方式与其他安全管理系统进行数据对接。

天眼系统每类告警外发功能均支持外发服务开关设置，可根据需要进行开启或关闭，以及对外发的告警数据进行灵活设置，包括系统日志、告警日志、原始告警日志、行为分析日志等。在 SYSLOG 方式外发配置支持 TCP 和 UDP 两种方式，并可灵活设置分隔符，并可配置多个 SYSLOG 接收服务器地址；SNMP 配置包含 SNMP 服务配置和 SNMP Trap 服务配置两个模块，用来对设备运行状态进行实时监测。管理员可通过 SNMP 客户端主动访问设备 MIB 库查询，也可通过配置 SNMP Trap 在客户端接收设备发出的 Trap 消息；邮件告警外发包括邮件服务信息配置、系统日志开关配置和告警日志开关配置三个模块可进行服务器使用协议、服务器地址、服务器端口、发件人、服务器认证开关、用户名、密码（邮箱服务器的密码）、SSL 等配置；KAFKA 对接外发告警支持设置 TOPIC、IP 及域名等信息，同时支持开启 kerberos 认证以保证数据的安全性验证。

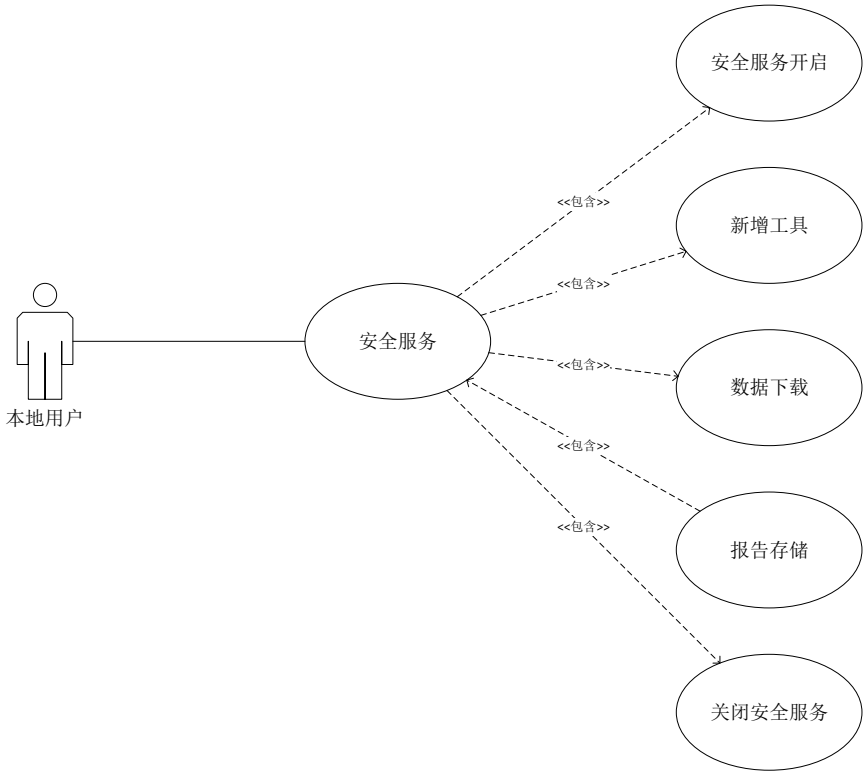
4.14 安全分析服务

安全分析服务分为三种场景：在线、半在线和离线，在线即云端可以直接连接客户环境的天眼环境；半在线则是云端无法直连客户环境，但是第三方电脑，可以连上云端，也可以连上客户环境；离线则是云端无法直连客户环境，也无法通过其他途径间接连上。

云端远程操作（在线和半在线）


Skyc2
命令转发
数据回传
分析平台
安全服务
数据下载
报告存储
<<包含>>
<<包含>>
云端用户

本地用户操作（离线）


安全服务开启
新增工具
数据下载
报告存储
关闭安全服务
安全服务
<<包含>>
<<包含>>
<<包含>>
<<包含>>
<<包含>>
本地用户

4.15 全包取证分析

天眼全包取证分析模块支持秒级提取海量历史流量，还原网络安全事件发生时的全部网络通讯内容，支持会话趋势展示，会话列表展示，会话协议树展示，并支持相关数据包的下载。

全包取证分析的场景可分为 5 部分：

全包取证：用户输入取证条件，页面展示命中条件的会话数随时间的变化趋势。

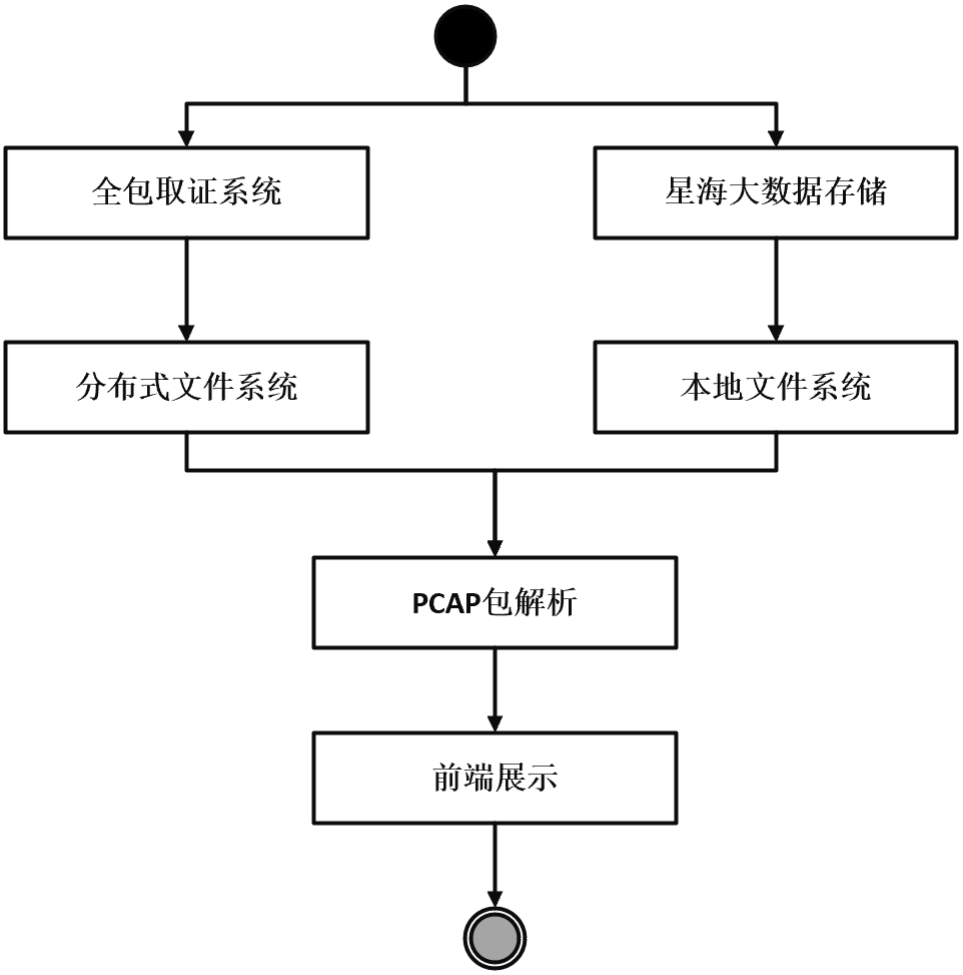
会话列表：用户选定数据包，并输入过滤条件，页面展示命中的会话列表。

会话协议树：用户选定会话，页面展示会话的协议树详情。

数据包下载：用户选定数据包，可进行单个会批量下载。

配置：用户配置分布式文件系统和取证系统。

从数据源提取目标流量，以 PCAP 包的形式存入文件系统，再经分析平台解析并展示。

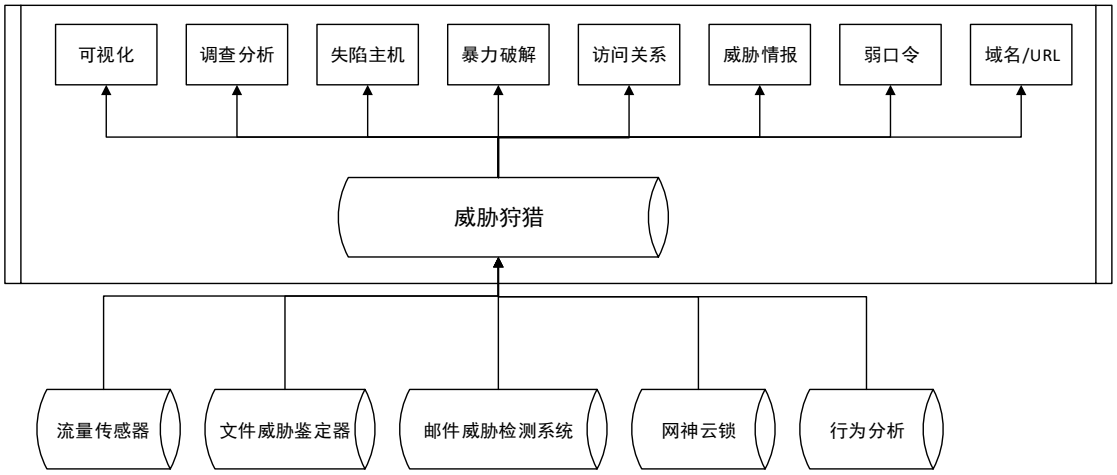


4.16 威胁狩猎

传统的防护设备只能对攻击行为进行告警，无法向用户描述整个攻击过程。天眼系统依据多年积累的经验从攻击链的维度将攻击行为进行重新划分，对告警进行深度关联分析，以告警中的受害主机为线索还原整个攻击过程（侦察-入侵-命令控制-横向渗透-数据外泄-痕迹清理）。

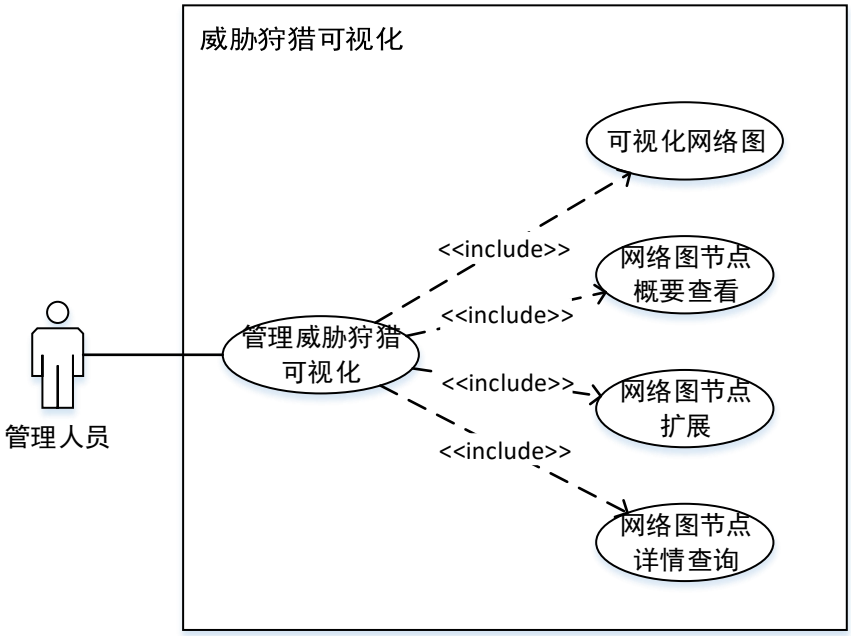
天眼系统运用先进的可视化呈现技术，支持与用户在可视分析画布上对任意线索的自定义拓线及溯源分析，该过程通过用户与系统的灵活交互对已有数据进行拓线分析，最终可以将威胁攻击的全过程推演并呈现在用户面前。同时，拓线分析过程支持结果快照导出，对于给定线索的溯源结果进行攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等维度的展示

威胁狩猎是将分析平台中告警，日志的信息进行汇总，进行多维度关联展示，可以有效的分析出数据之间的关联性，并获取相关的信息。



通过收集流量传感器，文件威胁鉴定器，邮件威胁检测系统，网神云锁数据，行为分析数据，对告警，资产，漏洞中的 IP，域名，文件 MD5，URI 等多种维度对数据进行分析

可视化图是通过图的方式展示告警和行为分析告警的数据，IP，域名，URI，邮箱和文件 md5 的关系。



4.17 运营管理

为提升系统的易用性，天眼系统提供多项便利的运营管理功能，主要包括：

- **平台名称及 logo 自定义**

天眼系统支持用户根据需要进行系统名称、系统 logo 等多种业务场景的自定义。

- **消息中心**

天眼系统的消息中心模块提供消息提醒能力，在天眼系统接收到重要告警数据、系统状态异常信息、主要进程异常信息、周期任务及数据下载时可以及时向用户发出声音和弹窗提醒。

消息中心支持个性化设置，对于告警日志可以进行威胁级别、攻击结果、告警类型的设置；对于系统状态信息可以进行 CPU、内存、硬盘故障、证书过

期的设置；对于主要进程监控可以数据库进程、关键日志、Redis 内存占用的设置；对于提示消息可以进行下载和任务的设置。

- **告警外发设置**

为满足企业用户不同安全管理系统之间数据同步的场景，天眼系统提供告警联动能力，支持通过 SYSLOG、SNMP、邮件、KAFKA 等多种方式与其他安全管理系统进行数据对接。

- **访问白名单设置**

为提高业务访问的安全性，天眼系统提供访问白名单设置和第三方登录账号管理，可灵活管理登录系统的用户范围。

- **系统规则管理**

天眼系统支持灵活的规则管理，主要包括：

- 威胁情报配置
- 白名单配置
- 弱口令字典配置
- 暴力破解规则配置
- 漏洞知识库配置
- 重点关注规则配置
- 特殊字段规则配置

5 典型部署

5.1 办公网环境下实施部署

5.1.1 办公网环境说明

部署奇安信天眼威胁发现与溯源的检测方案可以帮助用户及时有效的发现未知威胁，提升管理人员对未知威胁的发现速度和效率，最大限度的降低用户受攻击后的损失，回溯方案可以记录内网的任何一次网络行为为回溯提供强大的支撑。

办公网环境一般分为终端用户接入区、服务器区等，可以在每个区域分别部署天眼传感器，对不同区域中的流量进行全量检测和记录，可以将不同区域传感器还原的日志、文件发送给一个或多个分析平台集群。这样环境中所有网络行为都将以标准化的格式保存于天眼的分析平台，云端威胁情报和文件威胁鉴定器分析结果与本地分析平台进行对接，为用户提供基于情报和文件威胁鉴定器检测的威胁发现与溯源的能力。

部署该方案后，可以为用户解决以下安全问题：

1. 检测发现传统防护手段漏过的未知威胁。
2. 在隔离网络环境下检测未知威胁。
3. 对企业内的海量数据进行安全分析。
4. 对企业内已发现的问题进行攻击回溯。

5.1.2 所需带宽说明

天眼传感器对网络中的镜像流量会进行解析和全量还原，按照指定的格式生成日志传送至天眼分析平台或文件威胁鉴定器，还原后的文件会传送给文件威胁鉴定器。传感器生成的日志文件中对于镜像流量中的文件仅保留文件名称、文件类型等文件属性，不保留文件内容，文件内容由针对该文件生成的特

定 MD5 标签代替。经此处理后，天眼传感器向天眼分析平台传输日志时仅占用正常带宽的 3-4%。天眼传感器向天眼文件威胁鉴定器传输文件时占用带宽的 10%。

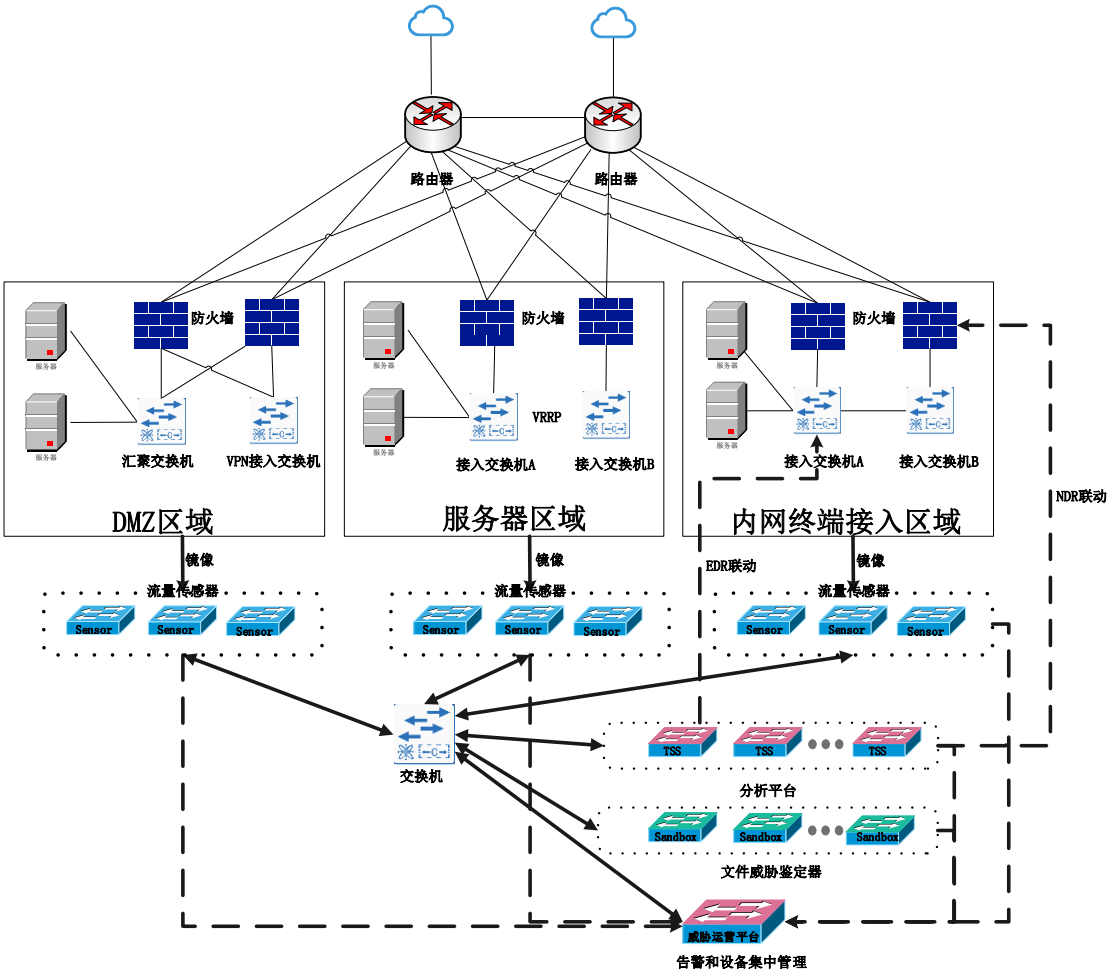
5.1.3 所需通信资源说明

结合实际部署的联动产品，天眼设备之间需要开放的端口如下：

操作平台	开放端口	传输协议	方向	服务	提供服务对象	端口用途说明
分析平台/沙箱/传感器	22	TCP（ssh）	双向	ssh	远程客户端	是远程访问控制的
分析平台/沙箱/传感器	443	TCP（HTTPS）	双向	https	远程客户端	web 访问端口(nginx 的访问端口）
分析平台/传感器	7755	TCP(SOCKET)	双向	TA	传感器	C 版本的 zmq 的接收端，protaocal_log,用于接收传感器的数据
分析平台/天擎	8855	TCP(SOCKET)	双向	skylar_log	天擎	skylar_log 也就是天擎日志接收的端口，用于接收天擎日志的数据
分析平台/沙箱	9955	TCP(SOCKET)	双向	TA	沙箱	python 版本的 zmq 的接收端，用于接收沙箱日志
分析平台	8098	TCP(SOCKET)	双向	星海大数据存储	上/下级分析平台	级联情况下，命令上下级加密同步
分析平台	8099	TCP(SOCKET)	单向	星海大数据存储	上/下级分析平台	级联情况下，下级数据加密同步到上级

分析平台/沙箱/传感器	161	UDP（SNMP）	单向	SNMP	SNMP 客户端	对外提供 SNMP 服务
分析平台/威胁运营平台	20611	Udp	双向	Syslog	威胁运营平台	分析平台 3084 与运营平台通过 syslog 传输告警
分析平台/威胁运营平台	9092	Tcp	双向	Kafka	威胁运营平台	分析平台 3091 与运营平台通过 kafka 传输告警
分析平台/威胁运营平台	9094	Tcp	双向	Kafka	威胁运营平台	分析平台 3091 与运营平台通过 kafka 传输告警

5.1.4 实施拓扑图



5.1.5 实施步骤说明

通用步骤：

1. 访问web：使用网线将PC的网口与分析平台的管理口eth0直连，在PC上使用谷歌浏览器，在地址栏中输入“https: //192.168.0.1”并回车（请注意，该地址是以https开头，而非http），然后出现web访问界面

2. 登陆对应产品平台系统配置页面进行如下基础配置

1）网络接口ip和路由和DNS配置

2）进行NTP 和snmp配置

3. 分析平台需要增加ES配置

4. 天眼设备之间的传输和联动配置

5. 对应离线更新各设备的规则包版本

具体步骤详见：天眼产品线各产品发布文档的上线指导手册说明

5.2 互联网侧实施部署

5.2.1 互联网侧说明

互联网侧天眼威胁发现与溯源的检测方案可以帮助用户及时有效的发现未知威胁，提升管理人员对未知威胁的发现速度和效率，最大限度的降低用户受攻击后的损失，回溯方案可以记录内网的任何一次网络行为为回溯提供强大的支撑。

互联网企业内网，一般分为办公网(DMZ 区)，生产网（企业的数据和业务统计区），外联区（企业对外提供服务区）； 在三个核心区域，可以在每一个区域的交换机上部署一套天眼设备；

办公区：主要可以使用天眼威胁感知系统，对内网中的非法访问，恶意文件上传和传播行为；资产主机漏洞风险，攻击流量行为特征进行实时发现和保留证据；

生产区（企业的数据和业务统计区）：主要可以使用天眼威胁感知系统，对核心资产的配置和漏洞进行检测，对核心资产的访问行为进行实时流量分析，对核心资产的弱口令，主机爆破，webshell 上传等最常见的攻击进行集中监测；

外联区： 主要可以使用天眼威胁感知系统，对外联的资产和域名，进行实时检测，利用情报，可以有效及时发现恶意访问或者恶意下载行为；对内外访问行为进行实时大屏监测展示，有效进行预警；

部署该方案后，可以为用户解决以下安全问题：

1. 检测发现传统防护手段漏过的未知威胁

2. 在隔离网络环境下检测未知威胁
3. 对企业内的海量数据进行安全分析
4. 对企业内已发现的问题进行攻击回溯

5.2.2 所需带宽说明

天眼传感器对网络中的镜像流量会进行解析和全量还原，按照指定的格式生成日志传送至天眼分析平台或沙箱，还原后的文件会传送给沙箱。传感器生成的日志文件中对于镜像流量中的文件仅保留文件名称、文件类型等文件属性，不保留文件内容，文件内容由针对该文件生成的特定 MD5 标签代替。经此处理后，天眼传感器向天眼分析平台传输日志时仅占用正常带宽的 3-4%。天眼传感器向天眼文件威胁鉴定器传输文件时占用带宽的 10%。

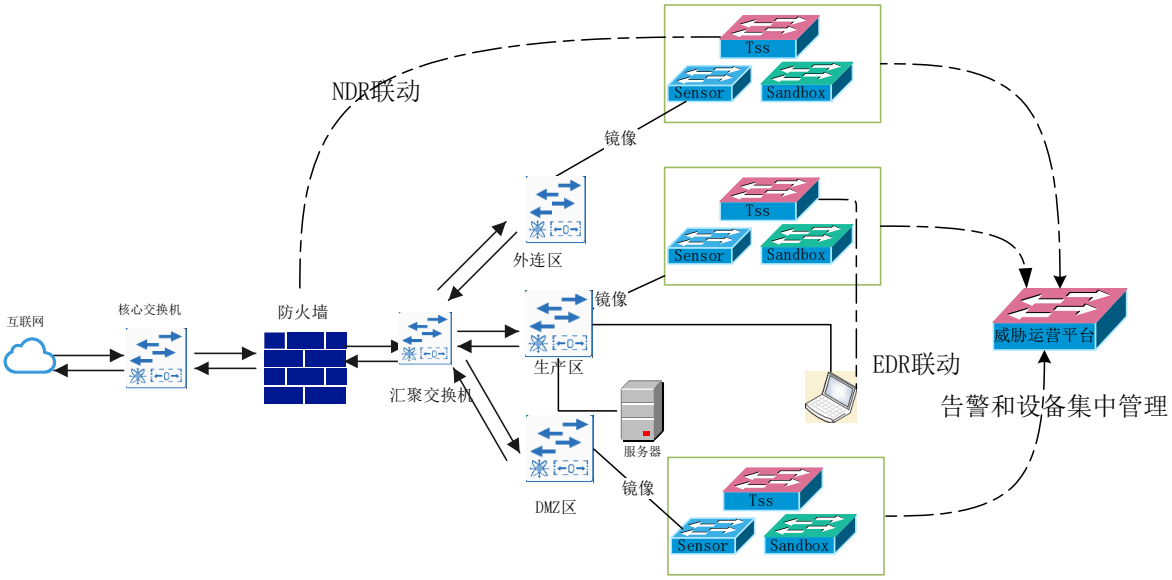
5.2.3 所需通信资源说明

结合实际部署的联动产品，天眼设备之间需要开放的端口如下：

操作平台	开放端口	传输协议	方向	服务	提供服务对象	端口用途说明
分析平台/沙箱/传感器	22	TCP（ssh）	双向	ssh	远程客户端	是远程访问控制的
分析平台/沙箱/传感器	443	TCP（HTTPS）	双向	https	远程客户端	web 访问端口(nginx 的访问端口)
分析平台/传感器	7755	TCP(SOCKET)	双向	TA	传感器	C 版本的 zmq 的接收端，protaocal_log,用于接收传感器的数据

分析平台/天擎	8855	TCP（SOCKET）	双向	skylar_log	天擎	skylar_log 也就是天擎日志接收的端口，用于接收天擎日志的数据
分析平台/沙箱	9955	TCP（SOCKET）	双向	TA	沙箱	python 版本的 zmq 的接收端，用于接收沙箱日志
分析平台	8098	TCP（SOCKET）	双向	星海大数据存储	上/下级分析平台	级联情况下，命令上下级加密同步
分析平台	8099	TCP（SOCKET）	单向	星海大数据存储	上/下级分析平台	级联情况下，下级数据加密同步到上级
分析平台/沙箱/传感器	161	UDP（SNMP）	单向	SNMP	SNMP 客户端	对外提供 SNMP 服务
分析平台/威胁运营平台	20611	Udp	双向	Syslog	威胁运营平台	分析平台 3084 与运营平台通过 syslog 传输告警
分析平台/威胁运营平台	9092	Tcp	双向	Kafka	威胁运营平台	分析平台 3091 与运营平台通过 kafka 传输告警
分析平台/威胁运营平台	9094	Tcp	双向	Kafka	威胁运营平台	分析平台 3091 与运营平台通过 kafka 传输告警

5.2.4 实施拓扑图



5.2.5 实施步骤说明

通用步骤：

1. 访问web：使用网线将PC的网口与分析平台的管理口eth0直连，在PC上使用谷歌浏览器，在地址栏中输入“https: //192.168.0.1”并回车（请注意，该地址是以https开头，而非http），然后出现web访问界面

2. 登陆对应产品平台系统配置页面进行如下基础配置

   1）网络接口ip和路由和DNS配置

   2）进行NTP 和snmp配置

3. 分析平台需要增加ES配置

4. 天眼设备之间的传输和联动配置

5. 对应离线更新各设备的规则包版本

具体步骤详见：天眼产品线各产品发布文档的上线指导手册说明

5.3 骨干网实施部署

5.3.1 骨干网说明

骨干网具有业务复杂、流量跨越多个网络区域、流量规模大等特点，为实现高速实时检测、及时全面透视骨干网中夹杂的攻击流量同时快速预警及溯源，需对骨干网分光流量进行分流并采用集群化部署，同时对集群性能、扩展能力、高可用性有设计要求。

5.3.2 所需带宽说明

天眼流量传感器对网络中的镜像流量会进行解析和全量还原，按照指定的格式生成日志传送至天眼分析平台或沙箱，还原后的文件会传送给沙箱。传感器生成的日志文件中对于镜像流量中的文件仅保留文件名称、文件类型等文件属性，不保留文件内容，文件内容由针对该文件生成的特定 MD5 标签代替。经此处理后，天眼传感器向天眼分析平台传输日志时仅占用正常带宽的 3-4%。天眼传感器向天眼文件威胁鉴定器传输文件时占用带宽的 10%。

5.3.3 所需通信资源说明

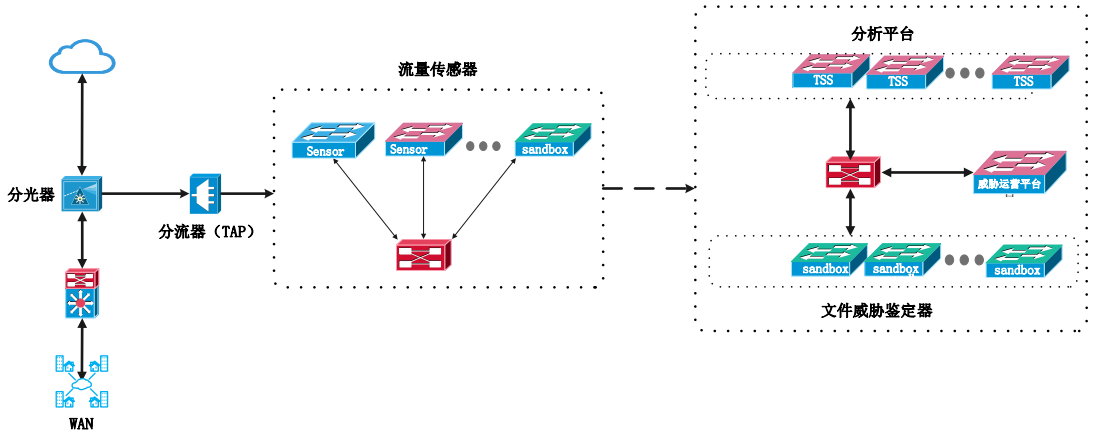
结合实际部署的联动产品，天眼设备之间需要开放的端口如下：

操作平	开放端口	传输协议	方向	服务	提供服务	端口用途说明

台					对象	
分析平台/沙箱/传感器	22	TCP（ssh）	双向	ssh	远程客户端	是远程访问控制的
分析平台/沙箱/传感器	443	TCP（HTTPS）	双向	https	远程客户端	web 访问端口(nginx 的访问端口）
分析平台/传感器	7755	TCP(SOCKET)	双向	TA	传感器	C 版本的 zmq 的接收端，protaocal_log,用于接收传感器的数据
分析平台/天擎	8855	TCP(SOCKET)	双向	skylar_log	天擎	skylar_log 也就是天擎日志接收的端口，用于接收天擎日志的数据
分析平台/沙箱	9955	TCP(SOCKET)	双向	TA	沙箱	python 版本的 zmq 的接收端，用于接收沙箱日志
分析平台	8098	TCP(SOCKET)	双向	星海大数据存储	上/下级分析平台	级联情况下，命令上下级加密同步
分析平台	8099	TCP(SOCKET)	单向	星海大数据存储	上/下级分析平台	级联情况下，下级数据加密同步到上级
分析平台/沙箱/传感器	161	UDP（SNMP）	单向	SNMP	SNMP 客户端	对外提供 SNMP 服务
分析平台/威胁运营平台	20611	Udp	双向	Syslog	威胁运营平台	分析平台 3084 与运营平台通过 syslog 传输告警
分析平	9092	Tcp	双向	Kafka	威胁运营	分析平台 3091 与运营平台

台/威胁运营平台					平台	通过 kafka 传输告警
分析平台/威胁运营平台	9094	Tcp	双向	Kafka	威胁运营平台	分析平台 3091 与运营平台通过 kafka 传输告警

5.3.4 实施拓扑图



5.3.5 实施步骤说明

通用步骤：

1. 访问web：使用网线将PC的网口与分析平台的管理口eth0直连，在PC上使用谷歌浏览器，在地址栏中输入“https：//192.168.0.1”并回车（请注意，该地址是以https开头，而非http），然后出现web访问界面

2. 登陆对应产品平台系统配置页面进行如下基础配置

1）网络接口ip和路由和DNS配置

2）进行NTP 和snmp配置

3. 分析平台需要增加对星海大数据存储的配置

4. 天眼设备之间的传输和联动配置

5. 对应离线更新各设备的规则包版本

具体步骤详见：天眼产品线各产品发布文档的上线指导手册说明

5.4 虚拟化环境实施部署

5.4.1 虚拟化环境说明

天眼虚拟化版本是运行在云平台虚拟化环境的天眼版本，由流量传感器、分析平台、沙箱组成，兼容主流云计算平台及虚拟化技术，支持自动化弹性部署、快速扩展等交付能力，与非虚拟化版本能力一致。

天眼虚拟化版本的流量传感器、分析平台、沙箱分别运行在各自虚拟机中，OpenStack+KVM/Xen 环境以 Docker 方式，VMware 平台以 ova 方式部署上云。

5.4.2 所需带宽说明

天眼传感器对网络中的镜像流量会进行解析和全量还原，按照指定的格式生成日志传送至天眼分析平台或沙箱，还原后的文件会传送给沙箱。传感器生成的日志文件中对于镜像流量中的文件仅保留文件名称、文件类型等文件属性，不保留文件内容，文件内容由针对该文件生成的特定 MD5 标签代替。经此

处理后，天眼传感器向天眼分析平台传输日志时仅占用正常带宽的 3-4%。天眼传感器向天眼文件威胁鉴定器传输文件时占用带宽的 10%。

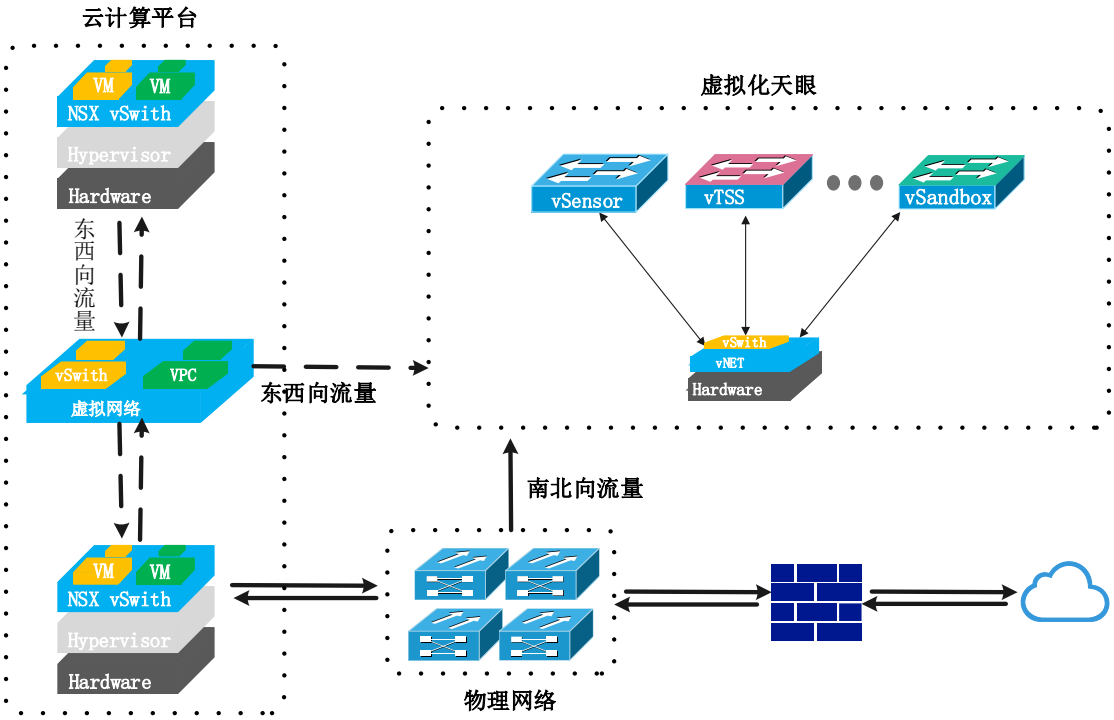
5.4.3 所需通信资源说明

结合实际部署的联动产品，天眼设备之间需要开放的端口如下：

操作平台	开放端口	传输协议	方向	服务	提供服务对象	端口用途说明
分析平台/沙箱/传感器	22	TCP（ssh）	双向	ssh	远程客户端	是远程访问控制的
分析平台/沙箱/传感器	443	TCP（HTTPS）	双向	https	远程客户端	web 访问端口(nginx 的访问端口)
分析平台/传感器	7755	TCP(SOCKET)	双向	TA	传感器	C 版本的 zmq 的接收端，protaocal_log,用于接收传感器的数据
分析平台/天擎	8855	TCP(SOCKET)	双向	skylar_log	天擎	skylar_log 也就是天擎日志接收的端口，用于接收天擎日志的数据
分析平台/沙箱	9955	TCP(SOCKET)	双向	TA	沙箱	python 版本的 zmq 的接收端，用于接收沙箱日志
分析平台	8098	TCP(SOCKET)	双向	星海大数据存储	上/下级分析平台	级联情况下，命令上下级加密同步
分析平台	8099	TCP(SOCKET)	单向	星海大数据存储	上/下级分析平台	级联情况下，下级数据加密同步到上级
分析平	161	UDP（SNMP）	单向	SNMP	SNMP 客户	对外提供 SNMP 服务

台/沙箱/传感器					端	
分析平台/威胁运营平台	20611	Udp	双向	Syslog	威胁运营平台	分析平台 3084 与运营平台通过 syslog 传输告警
分析平台/威胁运营平台	9092	Tcp	双向	Kafka	威胁运营平台	分析平台 3091 与运营平台通过 kafka 传输告警
分析平台/威胁运营平台	9094	Tcp	双向	Kafka	威胁运营平台	分析平台 3091 与运营平台通过 kafka 传输告警

5.4.4 实施拓扑图



5.4.5 实施步骤说明

通用步骤：

1. 访问web：使用网线将PC的网口与分析平台的管理口eth0直连，在PC上使用谷歌浏览器，在地址栏中输入“https：//192.168.0.1”并回车（请注意，该地址是以https开头，而非http），然后出现web访问界面

2. 登陆对应产品平台系统配置页面进行如下基础配置

   1）网络接口ip和路由和DNS配置

   2）进行NTP 和snmp配置

3. 分析平台需要增加对星海大数据存储的配置

4. 天眼设备之间的传输和联动配置

5. 对应离线更新各设备的规则包版本

具体步骤详见：天眼产品线各产品发布文档的上线指导手册说明

6 产品参数

6.1 分析平台

CPU	2*32 核 CPU（2 颗物理 CPU）
内存	256GB
存储(系统盘)	960G SSD
存储(数据盘)	12×8TB SATA
网口	4×千兆电口（含 2 个管理口）+ 4×万兆光口
扩展	6 个扩展槽位，可选配 4 千兆电口或 2 万兆光口网卡或 4 万兆光口网卡（不含光模块）
电源	冗余电源
尺寸	2U 机箱
性能	分析平台性能 60000 eps，日志处理速度不少于 90 万条每分钟；单台分析平台实际可处理流量 10Gbps

6.2 流量探针

CPU	1*8 核 CPU（1 颗物理 CPU）

内存	32GB
存储	1TB SATA
网口	6×千兆电口（含 2 个管理口） + 4×千兆光口（满配光模块）+流量镜像口 2 个万兆光口（满配光模块）+2 个万兆流量监听光口（满配光模块）
扩展	1 个扩展槽位，可选配 4 千兆电口、4 千兆光口、2 万兆光口、4 万兆光口网卡
电源	冗余电源
尺寸	1U 机箱
流量处理能力	1.5Gbps

7 产品优势与特点

7.1 首创使用互联网数据发掘 APT 攻击线索，提升企业对威胁看见的能力

传统的 APT 防护技术专注于从企业客户自身流量和数据中通过沙箱或关联分析等手段发现威胁。而由于企业网络防护系统缺少相关 APT 学习经验，而且攻击者的逃逸水平也在不断的进步发展，本地设备会经常性的出现误报和漏报现象，经常需要人工的二次分析进行筛选。而且由于 APT 攻击的复杂性和背景的特殊性，仅依赖于单一企业的数据经常无法有效的发现 APT 攻击背景，难以做到真正的追踪溯源。而天眼则创新性的从互联网数据进行发掘和分析，由于任何攻击线索都会有相关联的其他信息被互联网数据捕捉到，所以从互联网进行挖掘可极大提升未知威胁和 APT 攻击的检出效率，而且由于数据的覆盖面更大，可以做到攻击的更精准溯源。

7.2 以威胁情报形式打通攻击定位、溯源与阻断多个工作环节，帮助企业从源头上解决安全问题

传统的防护体系在多台设备间进行联动往往需要通过特别开发的接口对一种或几种特殊类别的告警或信息进行分发和通知，这种设计往往会制约多种不同设备或系统之间的信息传递。同时由于对于消息接口缺乏一个系统化的规范化的描述，很难对复杂的攻击行为进行准确定义。而天眼的一大创新点在于用威胁情报的形式对各种攻击中常出现的特点和背景信息进行记录和传输，而威胁情报将通过统一的规范化格式将攻击中出现的多种攻击特征进行标准化，可满足未来扩展攻击特征以及后续扩展联动设备的需要。

7.3 对告警进行深度分析以攻击链的视角重现攻击过程

传统的防护设备只能对攻击行为进行告警，无法向用户描述整个攻击过程以及给予相应的处置方案。天眼依据多年的积累经验从攻击链的维度将攻击行为进行重新划分，对告警进行深度调查分析，以告警中的受害主机为线索还原这个攻击过程（侦察-入侵-命令控制-横向渗透-数据外泄-痕迹清理）。同时结合安全专家积累的经验给出相应的处置方案。

7.4 结合企业业务对原始日志进行自动化深度分析，帮助企业发现可疑行为

传统的防护体系中是以固定的规则来匹配流量中的行为来告警，无法结合用户的业务来分析流量中的可疑行为。天眼结合安全专家积累的分析经验以企业业务为导向制定了多个自动化的分析场景，用来帮助企业发现自身的可疑行为。

7.5 支持分级部署对告警进行统一管理和分析

对于大型企业而言，单一的部署点已经无法满足整体运营管理需求。针对此场景，天眼支持级联部署将告警统一收集进行分析和展示。

7.6 高效的快速搜索技术帮助企业提升数据查找的能力

传统的安全方案中，对于企业本地数据的处理往往采用 mysql 等关系型数据库。这种设计早已不能满足当前数据量的处理性能需要。天眼创新性的采用搜索引擎技术作为本地数据存储和检索核心技术，采用 json 格式作为引擎的输入输出格式，这样可极大提高检索性能，可以为企业提供 TB 级的数据快速搜索能力，同时相比传统架构也能够降低大量接口上的开发量。天眼可为企业本地的大规模数据保存、攻击证据留存和查询、实时关联分析提供坚实的技术保障。

7.7 基于大数据挖掘分析的恶意代码智能检测技术，提升了客户检测恶意代码的能力

天眼采用了机器学习等人工智能算法，针对海量程序样本进行自动化分析，有效解决了大部分未知恶意程序的发现问题。由于传统杀毒技术严重依赖于样本获得能力和病毒分析师的能力，基本只能处理已知问题，不能对可能发生的问题进行防范，具有严重的滞后性和局限性。本技术对海量样本进行挖掘，能够找到恶意软件的内在规律，能对未来相当长时期的恶意软件技术做出前瞻性预测，实现不更新即可识别大量新型恶意软件，在全球处于领先水平。

7.8 基于轻量级沙箱的未知漏洞攻击检测技术，提升了客户检测未知漏洞的能力

现有的传统安全防护措施大多数使用基于签名（Signature）的机制对已知威胁进行检测和防护，而天眼的基于轻量级沙箱的未知漏洞攻击检测引擎是针对传统基于签名的局限性提出的解决方案，可以检测和发现主流客户端应用程序（IE/Office/AdobeReader）的可疑威胁，能对客户端应用中已知漏洞和未知 0day 漏洞的攻击利用进行检测。

7.9 专业的专家运营团队，全天候为企业保驾护航

为了推进自动化分析技术的发展，并对未知威胁做最终定性和跟踪，奇安信长时间维持了一个近百人的庞大安全分析团队，该团队技术能力覆盖了操作系统、逆向、漏洞挖掘、渗透等安全的各个技术领域，该团队成员的经验为云端分析系统的运行提供了宝贵输入，并支持了国内多次重大 APT 事件的深度挖掘和定位。奇安信的安全专家团队可为企业提供及时有效的安全服务，帮助企业保护自身网络的安全，减少企业遭受攻击时收到的损失。